

Next level access since 1833

SAG



SAFE-O-TRONIC® access

Handbuch

Möbelschließsysteme

SAFE-O-TRONIC access®

LSW

Hinweise zu diesem Dokument

© Copyright 2026 by Schulte-Schlagbaum AG

Navigeser Straße 100-110

D-42553 Velbert

Telefon +49 2051 2086-0

<http://www.sag-schlagbaum.com>

Ausgabe: 20260417

Version: 3.11

Dokumentennummer: 17.04.2026

Alle früheren Ausgaben verlieren mit dieser Ausgabe ihre Gültigkeit. Die Angaben in diesem Dokument können ohne vorherige Ankündigung geändert werden.



Hinweis: Weitergabe sowie Vervielfältigung dieses Dokuments, Verwertung und Mitteilung ihres Inhalts sind nicht gestattet, soweit nicht ausdrücklich zugestanden. Zuwiderhandlung verpflichtet zu Schadensersatz. Alle Rechte für den Fall der Patenterteilung oder Gebrauchsmuster-Eintragung vorbehalten.

Die Zusammenstellung der Informationen in diesem Dokument erfolgt nach bestem Wissen und Gewissen. Schulte-Schlagbaum AG übernimmt keine Gewährleistung für die Richtigkeit und Vollständigkeit der Angaben in diesem Dokument. Insbesondere kann Schulte-Schlagbaum AG nicht für Folgeschäden auf Grund fehlerhafter oder unvollständiger Angaben haftbar gemacht werden. Da sich Fehler, trotz aller Bemühungen, nie vollständig vermeiden lassen, sind wir für Hinweise jederzeit dankbar.

SAFE-O-TRONIC® und **SAFE-O-TRONIC access®** sind eingetragene Warenzeichen der Schulte-Schlagbaum AG.

- Dieses Dokument beschreibt die Inbetriebnahme und Bedienung eines **SAFE-O-TRONIC access®** Geräts (Definition siehe Deckblatt).
- Das Gerät darf nur für den vom Hersteller vorgesehenen Zweck verwendet werden.
- Dieses Dokument ist zugriffsfähig aufzubewahren.
- Unzulässige Veränderungen und die Verwendung von Ersatzteilen und Zusatzeinrichtungen, die nicht vom Hersteller des Gerätes verkauft oder empfohlen werden, können Brände, elektrische Schläge und Verletzungen verursachen. Solche Maßnahmen führen zu einem Ausschluss der Haftung, und der Hersteller übernimmt keine Gewährleistung.
- Reparaturen dürfen nur vom Hersteller durchgeführt werden.
- Für das Gerät gelten die Gewährleistungsbestimmungen des Herstellers in der zum Zeitpunkt des Kaufes gültigen Fassung. Für eine ungeeignete manuelle und automatische Erstellung von Parametern für ein Gerät, bzw. ungeeignete Verwendung eines Gerätes wird keine Haftung übernommen.
- Der Betreiber ist dafür verantwortlich, dass das Gerät nach anerkannten technischen Regeln im Aufstellungsland sowie anderen gültigen Vorschriften aufgestellt und angeschlossen wird.

Inhaltsverzeichnis

1	Systemüberblick	1
1.1	Bestimmungsgemäße Verwendung	1
1.1.1	Sicherheitshinweise	1
1.1.2	EU-Konformitätserklärung	2
1.2	Bedienelemente	2
1.2.1	Bluetooth low energy (BLE)	3
1.2.2	Kapazitive Tastatur	3
1.2.3	RFID Lesefeld	4
1.3	Einbaurichtungen	5
2	Montage und Inbetriebnahme	6
2.1	Montage	6
2.1.1	Vorbereitung der Türe	7
2.1.2	Montage Außeneinheit	7
2.1.3	Montage Inneneinheit	8
2.1.4	Montage SOT-WB	10
2.2	Abfrageschieber	10
3	Inbetriebnahme	12
3.1	Test Funktionen	12
3.1.1	TestCode	12
3.1.2	TestKey	12
3.1.3	TestCommand	13
3.2	Programmierung	13
3.2.1	Serien 200, 300 und 400	13
3.2.2	Serien 500, 600 und 600 LEGIC	13
3.3	Kalibrierung der internen Uhrzeit	13
3.3.1	Durchführung der Kalibrierung	14
4	Betriebsmodi	15
4.1	PIN Eingabe	15
4.2	Freie Schrankwahl	15
4.3	Feste Zuordnung	15
4.3.1	All-Open	16
4.3.2	One-Open	16
4.3.3	TGC	16
4.3.4	TSBC	16

5	Master Funktionen	18
5.1	Besonderheiten bei den Serien 200, 300 und 400	18
5.2	MasterKey	18
5.3	MasterCode	19
5.3.1	MasterCode eingeben	19
5.4	MasterCommand	19
5.4.1	MasterCommand nutzen	20
6	Datenstrukturen	21
6.1	Erläuterungen	21
6.1.1	Applikation	21
6.1.2	Ausweisnummer	21
6.1.3	KGEN	21
6.1.4	Gültigkeiten und Zeitpläne	22
6.1.5	Sicherheitspin	22
6.1.6	Berechtigung über Schließgruppen	22
6.1.7	Berechtigung über Schlossnummern	22
6.1.8	Berechtigung über Bereiche	22
6.1.9	Blacklist	22
6.1.10	Erlaubt mehrere Schlösser in freier Schrankwahl	23
6.1.11	Nutzungsdauer und Aktion am Ende der Nutzungsdauer	23
6.1.12	Datenspeicherung auf Transponder	23
6.2	Standard Generation 1	24
6.3	Standard Generation 2 - Allgemein	25
6.4	Freie Schrankwahl - Blocks	26
6.5	Freie Schrankwahl - Minimal	27
6.6	Freie Schrankwahl - Standard	28
6.7	Feste Zuordnung - Schließgruppen	29
6.8	Feste Zuordnung - Industrie	30
7	Funktionen	31
7.1	PIN-Codes	31
7.1.1	Sperre durch Falscheingaben	31
7.1.2	Aktivieren von Bluetooth	31
7.2	Automatische Aktionen	32
7.2.1	Dauer	32
7.2.2	Zeitpunkt	32
7.2.3	Öffnen	32
7.2.4	Sperren	32
7.3	Zeitzone	32
7.4	Zeitfunktionen	33
7.4.1	Gültig ab / bis / von-bis	33
7.4.2	Zeitpläne - Standard	33
7.4.3	Zeitpläne - Nutzungszeiten	34

7.4.4	Schedules - Usage times	34
8	Allgemeine Informationen	35
8.1	LED-Anzeige	35
8.1.1	LED-Anzeige Serie 200, 300 und 400	35
8.1.2	LED-Anzeige Serie 500, 600 und 600 LEGIC	37
8.2	Fehlerbehebung	44
8.3	Batterieüberwachung	44
8.3.1	Batteriewechsel	44
8.4	Austausch der Nummernplatte	45
8.5	Wartung und Pflege	45
8.6	Update der Firmware	45
8.6.1	Update bei Schlössern der Generation 1	46
8.6.2	Update bei Schlössern der Generation 2	46
9	Technische Daten	47
10	Technische Hinweise zu den Batterien und Batteriepacks	49
10.1	Baureihen und Batterielebensdauer	49
10.1.1	LS	49
10.1.2	LSW	49
10.1.3	DS	50
10.1.4	CS	50
10.1.5	DSH	50
10.2	Allgemeine Hinweise zur Batterielebensdauer	50
10.2.1	Schließsystemvariante	50
10.2.2	Transponder	51
10.2.3	Konfiguration und Nutzerverhalten	51
10.2.4	Hinweise zum Batteriewechsel	51
10.2.5	Entsorgung	51
	Abbildungsverzeichnis	52
	Tabellenverzeichnis	53

1 Systemüberblick

Möbelschlösser der Serie *SAFE-O-TRONIC access*® LSW sind alle mit verschiedenen Bedienelementen ausgestattet. Diese können je nach Variante und aktivierten Komponenten variieren. In diesem Handbuch wird immer von einem LSW in der vollen Ausbaustufe ausgegangen. Testfunktionen und Programmiermöglichkeiten unterscheiden sich zwischen den Serien 200, 300, 400 und den Serien 500, 600, 600 LEGIC.

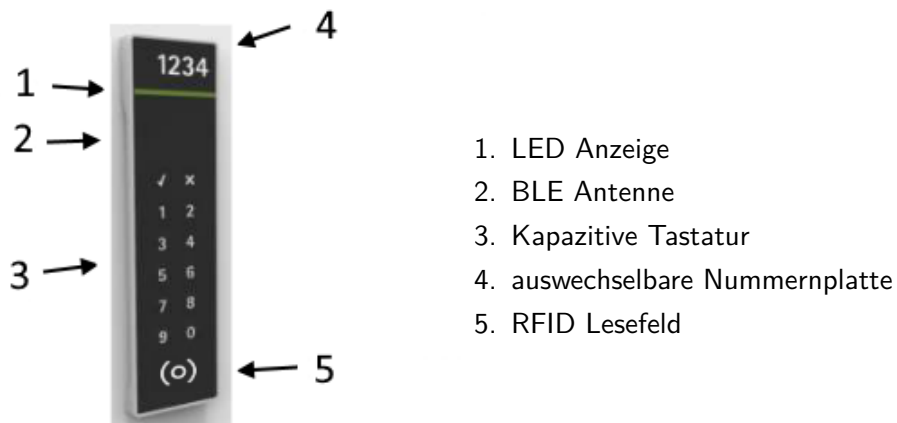


Abbildung 1.1 – LSW mit allen Funktionen

⚠ Hinweis: Das Aussehen und der Funktionsumfang kann, abhängig von der bestellten Variante, variieren.

1.1 Bestimmungsgemäße Verwendung

Das elektronische Möbelschließsystem *SAFE-O-TRONIC access*® LSW (LSW) ist für den Einbau in Möbel- oder Möbel- ähnlichen Aufbaute zum Verriegeln und Entriegeln vorgesehen. Das LSW Möbelschließsystem darf nur im Innenbereich eingesetzt werden.

1.1.1 Sicherheitshinweise

- An den Produkten der Schulte-Schlagbaum AG (SAG) sind keine Modifikationen irgendeiner Art, mit Ausnahme der in einer entsprechenden Anleitung beschriebenen, zulässig.
- Zur Vermeidung von Fehlfunktionen und Schäden sind nur Originalteile und Zubehör zu verwenden.

- Die Produkte dürfen nicht zum Verschluss von im Notfall lebensnotwendigen Hilfsmitteln verwendet werden. (z. B. Defibrillator, Notfallmedikamente und Feuerlöscher).
- Die Produkte dürfen nicht mit Farbe oder Säuren in Verbindung gebracht werden.
- Produkte nicht in explosionsgefährdeten Bereichen einsetzen.
- Die Produkte nur im definierten Temperaturbereich betreiben.
- Der Einbau sowie der Batteriewechsel darf nur durch geschultes Fachpersonal gemäß Anleitung durchgeführt werden.
- Es dürfen nur von SAG bezogene Batteriepacks verwendet werden.
- Batteriepacks dürfen nicht aufgeladen, kurzgeschlossen, geöffnet oder erhitzt werden.
- Alte bzw. verbrauchte Batteriepacks müssen fachgerecht entsorgt werden.
- Batteriepacks außerhalb der Reichweite von Kindern aufbewahren.
- Die Anleitung sollte von der den Einbau vornehmenden Person an den Benutzer weitergegeben werden.
- Für Beschädigungen an der Tür oder an den Bauteilen bei fehlerhafter Montage, übernimmt SAG keinerlei Haftung.
- Es wird keine Haftung bei fehlerhaft programmierten Einheiten übernommen. Treten Störungen, wie nicht möglicher Zugang zu verletzten Personen, Sachschäden oder sonstige Schäden auf, so haftet SAG nicht.

 **Hinweis: Wird ein programmiertes Schloss aus einer Anlage entwendet, kann dies zu einer Sicherheitsgefährdung der gesamten Schließanlage führen. Wenden sie sich in einem solchen Fall an SAG um ihre Anlage neu zu programmieren und die Sicherheitsgefährdung zu beheben.**

1.1.2 EU-Konformitätserklärung

Hiermit erklärt die Schulte-Schlagbaum AG, dass sich das Gerät in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinien 2014/53/EU sowie 2011/65/EU befindet. Die Langfassung der aktuellen CE-Konformitätserklärung finden Sie in englischer Sprache unter:

www.sag-schlagbaum.com/news/eu-konformitaet/

Schlösser der Serien 200, 300 und 400 sind bei der FCC unter dem IDENTIFIER Q3ILSW gelistet.

1.2 Bedienelemente

Die Tabelle 1.1 zeigt eine Übersicht, welche Bedienelemente in den jeweiligen Schlossvarianten grundsätzlich vorhanden sind. Die Aktivierung kann jedoch von der gekauften Lizenz abhängig sein.

Die RFID Funktion steht bei der Serie 200 nur dem Betreiber für administrative Zwecke zur Verfügung.

Tabelle 1.1 – Übersicht über die verschiedenen Bedienelemente

Schlossvariante	BLE	kapazitive Tastatur	RFID MIFARE	RFID LEGIC
200		×	[×	
300			×	
400		×	×	
500	×	×		
600	×	×	×	
600 LEGIC	×	×	×	×

1.2.1 Bluetooth low energy (BLE)

Schlösser der Serien 500, 600 und 600 LEGIC verfügen alle über ein Bluetooth low energy Interface (Bluetooth Version 4.2). Dieses kann mit den SAG eigenen Apps angesprochen werden. Die Reichweite des BLE wurde auf ca. 3m begrenzt.

1.2.2 Kapazitive Tastatur

Die kapazitive Tastatur verfügt über 12 oder 13 Tasten, die 10 Zifferntasten und zwei oder drei zusätzliche Funktionstasten. Die einzelnen Funktionen sind in Tabelle 1.2 aufgeführt.



Hinweis: Die kapazitive Tastatur kann nicht mit Handschuhen bedient werden

Tabelle 1.2 – Übersicht über die verschiedenen kapazitiven Tasten

Taste	Bezeichnung	Funktion
	OK	Abschluss einer Codeeingabe
	Abbruch	Codeeingabe wird abgebrochen, alle Eingaben werden gelöscht
	Bluetooth	Aktiviert die BLE-Schnittstelle zur Datenübermittlung (nur ab Serie 500)
	Nummerntasten	Eingabe einer Ziffer eines Codes

Wird zwischen dem Betätigen der einzelnen Tasten eine Pause von mehr als drei Sekunden gemacht,

wird die komplette Eingabe abgebrochen.

Ansonsten sind die Hinweise zur PIN-Eingabe im Kapitel 7.1 zu beachten.

1.2.3 RFID Lesefeld

Das RFID Lesefeld liegt im unteren Bereich des Schlosses (Einbaurichtung A, siehe Kapitel 1.3). Es umfasst die Tasten 9, 0 und Bluetooth. Für eine möglichst schnelle und sichere Lesung der RFID Daten muss eine möglichst große Antennenüberlagerung zwischen Schloss und RFID Transporter erreicht werden. Bei Coin Transpondern ist dies bei einer mittigen Annäherung am besten gegeben. Bei Karten Transpondern sollte eine Ecke der Karte in das Lesefeld gehalten werden.



Abbildung 1.2 – LSW mit RFID Lesefeld (rot) und Transponderkarte (grün)

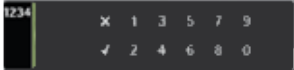
1.3 Einbaurichtungen

Je nach Schranktyp können die Schlösser der Serie LSW in verschiedenen Einbaurichtungen montiert werden.

⚠ Hinweis: In diesem Handbuch wird exemplarisch immer von der Einbaurichtung A ausgegangen

⚠ Hinweis: Schlösser müssen, sofern sie über eine Tastatur verfügen, in der richtigen Einbaurichtung bestellt werden.

Tabelle 1.3 – Übersicht über die verschiedenen Einbaurichtungen

Einbaurichtung A		Einbaurichtung B	
	Nummernplatte oben		Nummernplatte unten
Einbaurichtung C		Einbaurichtung D	
	Nummernplatte links		Nummernplatte rechts

2 Montage und Inbetriebnahme

Dieses Kapitel beschreibt die Montage der Schlösser der Serie *SAFE-O-TRONIC access*[®] LSW am Schrank und die notwendigen Vorbereitungen der Türe.

2.1 Montage

Die Schlösser der Serie LSW bestehen immer aus zwei Komponenten. Beide Komponenten sind mit einem Kabel mit einander verbunden. Die Montage muss immer in der folgenden Reihenfolge erfolgen:

1. Vorbereitung der Türe mit den notwendigen Löchern
2. Montage der Außeneinheit
3. Montage der Inneneinheit
4. Verbindung beider Einheiten durch einstecken des Verbindungskabels in der Inneneinheit
5. Funktion des LSW bei geöffneter Tür testen (siehe Kapitel 3.1).
6. Funktion bei geschlossener Tür testen. Hier ist besonders auf eine Leichtgängigkeit des Riegels und die korrekte Funktion des Abfrageschiebers zu achten. Das automatische Öffnen wird nur gewährleistet wenn der Riegel bei geschlossener Tür leichtgängig zu bewegen ist.

2.1.1 Vorbereitung der Türe

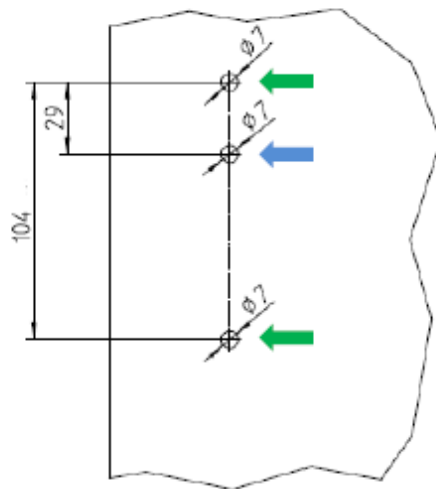


Abbildung 2.1 – Notwendige Löcher für die Außeneinheit

Für die Montage des Außengehäuses werden drei Löcher mit einem Durchmesser von 7mm benötigt. Die beiden äußeren Löcher (grün) dienen zur Befestigung der Außeneinheit. Das mittlere Loch (blau) wird zur Durchführung des Verbindungskabels benötigt.

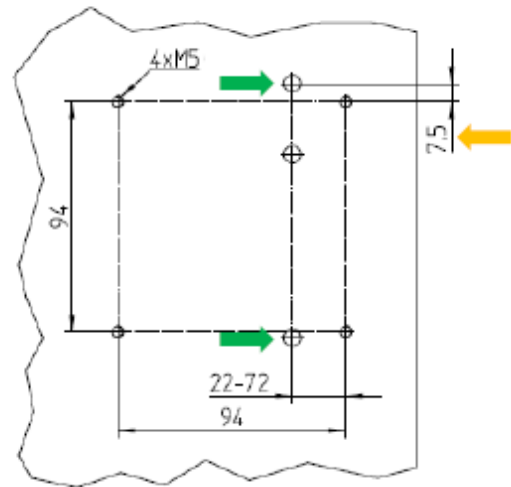


Abbildung 2.2 – Notwendige Löcher für die Inneneinheit

Da die Schraubenköpfe auf der Türinnenseite vom Innengehäuse abgedeckt werden, müssen die Löcher zur Montage des Außengehäuses in der Höhe zu den Befestigungsbohrungen des Innengehäuses gebohrt werden. Die seitliche Lage des Außengehäuses muss im Bereich von 22-72mm liegen.

⚠ Hinweis: Die vertikale Ausrichtung der Bohrungen von Innen- und Außeneinheit sind sehr wichtig. Wird dieses Maß (gelb) nicht eingehalten, können die Schraubenköpfe der Außeneinheit Druck auf die Mechanik der Inneneinheit ausüben und damit die Funktion beeinträchtigen oder sogar zum versagen der Inneneinheit führen.

2.1.2 Montage Außeneinheit

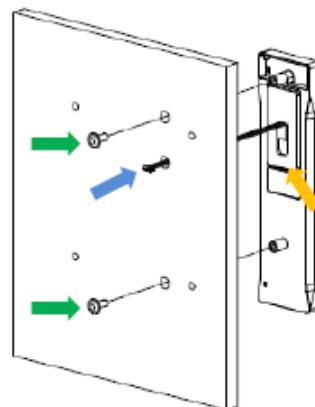


Abbildung 2.3 – Montage der Außeneinheit

Bei der Montage der Außeneinheit sind folgende Schritte durchzuführen:

1. Richtige Schraubenlänge anhand der Türstärke auswählen (siehe Tabelle 2.1).
2. Kabel durch das mittlere Loch führen.
3. Außeneinheit mit den beiden Bolzen in die dafür vorgesehenen Löcher positionieren. Beim Einsetzen darauf achten, dass das Kabel nicht eingequetscht und vollständig durch das Loch durch gezogen wird.
4. Außeneinheit mit den beiden Schrauben verschrauben.

⚠ Hinweis: Die Schrauben M4x20 und M4x25 sind keine Standardlängen und müssen bei der Bestellung gesondert bestellt werden.

Tabelle 2.1 – Übersicht über die richtige Schraubenlänge abhängig von der Türstärke

Türstärke [mm]	Schrauben (je 2 Stück)
10-15	M4x10
16-21	M4x16
22-25	M4x20
26-30	M4x25

⚠ Hinweis: Falsche Schraubenlängen können zur Beschädigung des Außengehäuses führen.

⚠ Hinweis: Um den IP-Schutz zu gewährleisten, muss die Dichtung (gelb) vollflächig an der Türe anliegen.

2.1.3 Montage Inneneinheit

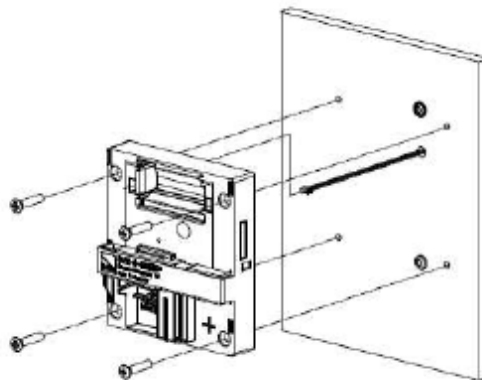


Abbildung 2.4 – Montage der Inneneinheit

Für die Montage des Innengehäuses werden vier Befestigungsschrauben benötigt. Die Ausführung der Befestigungsschrauben hängt von dem vorhandenen Türmaterial ab. Standardmäßig werden für die Befestigung des Innengehäuses Schrauben M5x25 eingesetzt. Zur Befestigung des Innengehäuses werden vier Gewinde (-hülsen) M5 in der Tür benötigt.

⚠ Hinweis: Die Schrauben dürfen maximal mit einem Drehmoment von 2,5 Nm angezogen werden.

Bei der Montage der Außeneinheit sind folgende Schritte durchzuführen:

1. Verbindungskabel durch eine der beiden Kabeldurchführungen in der Inneneinheit führen
2. Inneneinheit an die Türe setzen. Dabei ist darauf zu achten, dass das Kabel nicht eingequetscht und vollständig durch die Kabeldurchführungen durch gezogen wird. Außerdem ist darauf zu achten, dass die Schraubenköpfe der Außeneinheit in den dafür vorgesehenen Vertiefungen der Inneneinheit sitzen.
3. Inneneinheit mit vier Schrauben verschrauben.

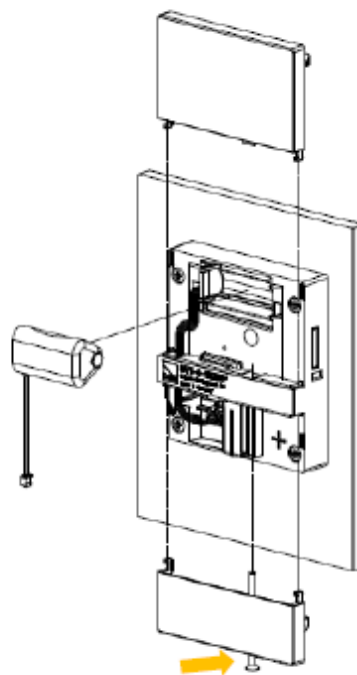


Abbildung 2.5 – Montage der Inneneinheit

Nachdem die beiden Einheiten befestigt worden sind, sind noch einige letzte Schritte auszuführen:

1. Verbindungskabel durch das Loch auf der linken Seite führen.
2. Batterie einsetzen und das Batteriekabel durch das gleiche Loch führen
3. Verbindungskabel in den 6 poligen Stecker einstecken. Dabei ist darauf zu achten, dass der Stecker grade eingeführt wird um Beschädigungen zu vermeiden.
4. **NUR BEI ONLINE ANLAGEN (200, 300 und 400):** Funkmodul SOT-WB in den Schlitz oberhalb der beiden Steckverbinder einführen und ganz nach unten drücken. Bitte berücksichtigen

sie die Hinweise in Kapitel 2.1.4.

5. Batteriekabel in den 2 poligen Stecker einstecken. Dabei ist darauf zu achten, dass der Stecker grade eingeführt wird um Beschädigungen zu vermeiden.
6. Oberen Deckel auf die Inneneinheit setzen
7. Unteren Deckel auf die Inneneinheit setzen
8. Batterieschraube (gelb) TX20 festschrauben, um die beiden Deckel zu fixieren

2.1.4 Montage SOT-WB



Abbildung 2.6 – Montage der Inneneinheit



⚠ Hinweis: Beachten Sie die Handhabungsvorschriften zum sicheren Umgang mit Elektronikbauteilen. ESD Schutz beachten!

2.2 Abfrageschieber

Die Möbelschlösser der Baureihe LSW sind mit einem Abfrageschieber zur Türkontrolle ausgerüstet. Dieser gefederte Abfrageschieber wird auf beiden Seiten des Innenschlosses mit den Riegeln ausgefahren. Um eine verschlossene Tür sicher zu erkennen muss der Abfrageschieber minimal 4mm vom Rahmen (oder Schließblech) eingedrückt werden. Bei einer geschlossenen Tür darf der Abfrageschieber auf der Seite des aktiven Riegels minimal 1mm und maximal 8mm ausgefahren sein (siehe Abbildung 2.7).

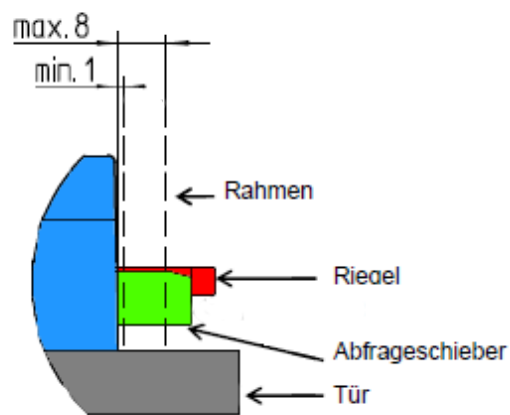


Abbildung 2.7 – Rahmenposition (gestrichelt) für die korrekte Funktion des Abfrageschiebers.
Riegel (rot), Abfrageschieber (grün), Türe (grau) und Schloss (blau)

⚠ Hinweis: Der Abfrageschieber signalisiert unabhängig von der Riegelstellung den Status der Tür. Dieser Status wird u.a. für die Türüberwachung und Alarmmeldung benötigt. Die Funktionalität des Abfrageschiebers kann konfiguriert werden. Hinweise zu den Konfigurationsmöglichkeiten entnehmen sie bitte dem Handbuch der Programmiersoftware.

⚠ Hinweis: Der Abfrageschieber ist bis zur Programmierung deaktiviert. Bei Verwendung der Test Funktionen kann die korrekte Funktion des Abfrageschiebers daher nicht getestet werden.

3 Inbetriebnahme

Bei Auslieferung sind alle Schlösser im Werkszustand. Dabei sind die Testfunktionen TestCode (PIN), TestKey (RFID) und TestCommand (BLE) aktiv. Diese werden mit der Programmierung der Schlösser deaktiviert. Zur Inbetriebnahme der Schlösser der Serie *SAFE-O-TRONIC access*® LSW ab Serie 500 ist die *LockManager* (ab Version 7) oder eine separat erhältliche Initialisierungsdatei erforderlich. Die Serien 200, 300 und 400 können auch mit einem *LockManager* Version 6 oder einem ProgKey-Set in Betrieb genommen werden.

Die Programmierung ist in einem separaten Handbuch beschrieben.

3.1 Test Funktionen

Mit den Testfunktionen TestCode (PIN), TestKey (RFID Transponder) und TestCommand (BLE Befehl) können die Schlösser nach der Montage getestet werden.

Die Test Funktionen können nur in Abhängigkeit von der Schlossserie genutzt werden. Eine Übersicht ist dem entsprechenden Handbuch zu entnehmen.

 **Hinweis: Es ist besonders auf die Leichtgängigkeit der mechanischen Bauteile beim Verschließen zu achten. Bei einem verspannten Einbau kann es zu Funktionsstörungen kommen.**

 **Hinweis: Alle Testfunktionen bleiben bis zur Programmierung der Schlösser aktiv**

3.1.1 TestCode

Der TestCode besteht aus den Tasten  und .

1.  Taste 0 betätigen
2.  Taste OK betätigen
3. Schloss führt eine Riegelfahrt aus

3.1.2 TestKey

Der TestKey wird wie jeder andere Transponder vor das Lesefeld des Schlosses gehalten. Dabei sind die Hinweise des Handbuchs zu beachten. Das Schloss gibt nach dem erfolgreichen Lesen des Transponders die Betätigung frei.

Das Schloss führt nach dem erfolgreichen Lesen des Transponders eine Riegelfahrt durch. Zum Öffnen des Schlosses wird der TestKey erneut vor das Schloss gehalten. Der Riegel muss automatisch wieder zurück in die Ausgangsstellung fahren. Ist dies nicht der Fall, muss die Leichtgängigkeit des Riegels überprüft werden.

 **Hinweis: Abhängig von der Schlossserie und der Firmware-Version sind unterschiedliche TestKeys erforderlich. Bitte wenden sie sich bei Fragen an die Hotline.**

3.1.3 TestCommand

Um den TestCommand nutzen zu können, ist die SAG Management App (SAM) notwendig. Bevor der Befehl übertragen werden kann, muss die Bluetooth Kommunikation mit der Taste  aktiviert werden. Dies ist vor jeder Befehlsübermittlung notwendig.

1. Bluetooth wie im Kapitel 7.1.2 beschrieben aktivieren Die blaue LED blinkt.
2. TestCommand in der SAG Management App (SAM) auswählen und abschicken
3. Warten, bis die SAG Management App (SAM) die Bluetooth Verbindung aufgebaut hat
4. Schloss führt eine Riegelfahrt aus

3.2 Programmierung

Die Programmierung ist in einem separaten Handbuch beschrieben.

3.2.1 Serien 200, 300 und 400

Die Programmierung der *SAFE-O-TRONIC access*[®] Schlösser erfolgt über die LockManager Software (ab Version 6) und das SystemKey-Set.

Alternativ kann auch ein ProgKey-Set für die Programmierung genutzt werden.

3.2.2 Serien 500, 600 und 600 LEGIC

Die Programmierung der *SAFE-O-TRONIC access*[®] Schlösser erfolgt über die LockManager Software (ab Version 7) und die Bluetooth SAG Management App (SAM).

Alternativ kann auch eine vorkonfigurierte Initialisierungsdatei verwendet werden. Diese sind bei SAG in bestimmten Konfigurationen erhältlich.

3.3 Kalibrierung der internen Uhrzeit

 **Hinweis: Eine Kalibrierung kann nur bei Schlössern der Serien 500, 600 und 600 LEGIC durchgeführt werden.**

Durch die Kalibrierung der internen Uhrzeit kann diese deutlich genauer betrieben werden. Die Kalibrierung ist nicht notwendig wenn

1. Eine Anlage mit CLW betrieben wird - Uhrzeiten werden hier täglich per Funk synchronisiert
2. Eine Anlage keine Funktionen mit einer festen Uhrzeit (z.B. TGC oder automatische Öffnung) nutzt

Ohne Kalibrierung sind Abweichungen der Uhrzeit von mehreren Minuten je Monat möglich. Die Kalibrierung reduziert diese Abweichungen auf wenige Sekunden pro Jahr.

3.3.1 Durchführung der Kalibrierung

 **Hinweis: Eine Kalibrierung kann erst durchgeführt werden, wenn die Anlage mindestens 4 Wochen betrieben worden ist.**

Um eine Kalibrierung der Uhrzeit durchführen zu können muss der folgende Ablauf eingehalten werden.

1. Installation und Inbetriebnahme der Anlage über die SAG-App
2. Betrieb der Anlage für mindestens 4 Wochen
3. Aktivierung der Bluetooth Funktion am Schloss (siehe Kapitel 7.1.2)
4. Ausführen des Befehls Uhr kalibrieren in der SAG-App
5. Optische Rückmeldung des Schlosses abwarten

4 Betriebsmodi

Die Schlösser der Serie *SAFE-O-TRONIC access*[®] LSW können in unterschiedlichen Betriebsmodi genutzt werden. Alle Betriebsmodi, mit Ausnahme der Betriebsart TGC, sind mit allen Betätigungsvarianten (PIN, RFID, BLE) verfügbar. Die unterschiedlichen Betätigungsvarianten werden im Kapitel 1.2 beschrieben. TGC benötigt immer die Betätigungsvariante PIN.

4.1 PIN Eingabe

1. Tasten     betätigen
2.  Taste OK betätigen
3. Schloss führt eine Riegelfahrt aus

 **Hinweis: 2 4 3 5 ist nur ein Beispielcode**

 **Hinweis: Die Länge des UserPINs kann in den Schlosseinstellungen im LockManager verändert werden (4 bis 6-stellig)**

 **Hinweis: Die Bestätigung mit der Taste OK ist in einigen Betriebsarten nicht, oder nur beim Verschließen notwendig. In diesen Betriebsarten gibt das Schloss nach der Eingabe der letzten Ziffer die Betätigung frei.**

4.2 Freie Schrankwahl

Ein Schloss in der Betriebsart „Freie Schrankwahl“ kann durch einen beliebigen UserCode (PIN), UserKey (RFID) oder UserCommand (BLE) verschlossen werden. Der UserCode kann vom Nutzer frei gewählt werden. UserKey und UserCommand müssen für die Anlage vorher im LockManager (ab Version 7) erstellt werden und können anschließend an einem frei wählbaren Schloss genutzt werden. Der UserKey muss nach dem anlegen im LockManager zusätzlich beschrieben werden. Beim UserCommand muss dieser an die SAG User App oder die verwendete Fremdapp übermittelt werden.

4.3 Feste Zuordnung

Bei der festen Zuordnung muss das Schloss oder der Transponder mit den schließberechtigten UserDaten programmiert werden. Die feste Zuordnung kann in unterschiedlichen Varianten genutzt werden. Diese werden im folgenden beschrieben.

4.3.1 All-Open

In der Betriebsart All-Open können alle UserDaten, die dem Schloss bekannt sind, das Schloss betätigen. Dabei ist es egal, welche UserDaten das Schloss vorher benutzt haben.

Beispiel: Nutzer A verschließt das Schloss mit seinem UserKey. Nutzer B öffnet das Schloss mit seinem UserKey.

Der Betriebsmodus ist immer dort sinnvoll, wo verschiedene Nutzer ein Schloss betätigen müssen. Ein Beispiel sind Medikamentenschränke im Krankenhaus oder Türanwendungen.

4.3.2 One-Open

In der Betriebsart One-Open können nur die UserDaten den Schrank wieder öffnen, die diesen vorher verschlossen haben. Die UserDaten müssen dem Schloss bekannt sein.

Beispiel: Nutzer A verschließt das Schloss mit seinem UserKey. Nur Nutzer A kann das Schloss mit seinem UserKey wieder öffnen.

Der Betriebsmodus ist immer dort sinnvoll, wo ein Nutzer einen Schrank nutzt. Ein Beispiel sind Umkleideschränke in einem Betrieb.

4.3.3 TGC

Der TGC besteht aus zwei PIN Codes. Der erste Code ist der StartCode. Dieser Code ist 7 bis 12 stellig und muss immer bei der ersten Benutzung durch einen Nutzer eingegeben werden. Der Code enthält alle notwendigen Informationen für das Schloss, wie zum Beispiel die Nutzungsdauer. Der zweite Code ist der ComfortCode. Dieser Code ist immer 4 stellig und abhängig vom StartCode. Der ComfortCode kann nach der erstmaligen Eingabe des StartCodes verwendet werden, solange dieser gültig ist.

TGC ist ab der Serie 400 nutzbar.

4.3.4 TSBC

 **Hinweis: TSBC ist ab der Serie 500 mit Firmware 03.04.01 nutzbar.**

Ein TSBC besteht aus zwei PIN Codes. Der erste Code ist der StartCode. Dieser Code ist 7 bis 12 stellig und muss immer bei der ersten Benutzung durch einen Nutzer eingegeben werden. Der Code enthält alle notwendigen Informationen für das Schloss, wie zum Beispiel die Nutzungsdauer. Der zweite Code ist der ComfortCode. Dieser Code ist immer 4 stellig und abhängig vom StartCode. Der ComfortCode kann nach der erstmaligen Eingabe des StartCodes verwendet werden, solange dieser gültig ist.

Der TSBC kann in unterschiedlichen Betriebsmodi genutzt werden. Der Betriebsmodus ist im TSBC enthalten und kann daher frei pro Code gewählt werden. Die unterstützten Betriebsmodi werden in den kommenden Unterkapiteln erläutert.

 **Hinweis: Unabhängig von der Betriebsart (One open oder All open) können ALLE gültigen TSBC-Codes ein Schloss öffnen. Dabei ist es egal, mit welchem Code das Schloss verschlossen worden ist. Im Modus One open kann ein mit einem TSBC verschlossenes Schloss nur mit einem TSBC-Code oder einem MasterCode geöffnet werden.**

 **Hinweis: Identische Codes werden, nach dem ihre Berechtigung abgelaufen ist, immer abgelehnt.**

TSBC - Betätigungen

Im Betriebsmodus Betätigung gibt es unterschiedliche Möglichkeiten (Sub-Betriebsmodi) einen TSBC zu generieren.

1. Öffnen - Der Code ist nur zum einmaligen Öffnen eines Schlosses berechtigt
2. Schließen - Der Code ist nur zum einmaligen Verschließen eines Schlosses berechtigt
3. Betätigungen - Der Code ist für bis zu 7 Betätigungen am Schloss (egal ob öffnen oder verschließen) berechtigt

Alle Codes sind nur an dem Tag gültig, für den sie generiert werden.

 **Hinweis: Pro Tag können maximal 16 Codes erzeugt werden. Die Codes können parallel in Verwendung sein.**

TSBC - Stunden

Im Betriebsmodus Stunden wird ein TSBC generiert, der für eine Anzahl von bis zu 63 Stunden gültig ist. Die Gültigkeit beginnt zu der im Code angegebenen Stunde (nur volle Stunden möglich) am angegebenen Tag.

Beispiel: Code ab 03.02.2025 14:00 für 26 Stunden

Gültigkeitsbeginn: 03.02.2025 14:00

Gültigkeitsende: 04.02.2025 15:59

 **Hinweis: Pro Tag können maximal 16 Codes erzeugt werden. Die Codes können parallel in Verwendung sein.**

TSBC - Tage

Im Betriebsmodus Tage wird ein TSBC generiert, der für eine Anzahl von bis zu 1024 Tage gültig ist. Die Gültigkeit beginnt am angegebenen Tag um 00:00 und endet nach der Anzahl der angegebenen Tage um 23:59.

Beispiel: Code ab 03.02.2025 für 5 Tage

Gültigkeitsbeginn: 03.02.2025 00:00

Gültigkeitsende: 07.02.2025 23:59

 **Hinweis: Pro Tag können maximal 16 Codes erzeugt werden. Die Codes können parallel in Verwendung sein.**

5 Master Funktionen

Dieses Kapitel beschreibt die Master Funktionen bei den Schlössern *SAFE-O-TRONIC access®* LSW. Abhängig von den aktivierten Funktionen können einzelne Funktionen nicht verfügbar sein. Es ist jedoch immer mindestens eine MasterFunktion verfügbar.

5.1 Besonderheiten bei den Serien 200, 300 und 400

Bei den Serien 200, 300 und 400 wird zwischen MasterKey 1 und 2 unterschieden. Das gleiche gilt auch für den MasterCode. Zur besseren Lesbarkeit wird hier nur der MasterKey beschrieben, des Verhalten beim MasterCode ist identisch.

Der MasterKey 1 dient nur dem Öffnen von Schränken. Ein Verschließen ist mit diesem Key nicht möglich. Das geöffnete Schloss bleibt anschließend gesperrt und kann nicht mehr mit einem User Medium genutzt werden. Die Nutzung ist erst nach Aufhebung der Sperre durch den MasterKey 2 möglich.

5.2 MasterKey

Der MasterKey kann jederzeit zum Betätigen eines Schlosses oder zum Freigeben einer Sperre verwendet werden.

Ein MasterKey muss für seinen Einsatz in der LockManager Software vor der Benutzung programmiert werden. Folgende Parameter können eingestellt werden:

1. Schosnummer oder Schlossnummernbereich (örtliche Berechtigung)
2. Gültigkeit von, Gültigkeit bis (zeitliche Berechtigung)

So ist es möglich die MasterKeys nur für ein bestimmtes Schloss oder Schlossbereich und zusätzlich auch noch in einem bestimmten Zeitraum freizugeben.

Auf dem MasterKey werden die letzten Benutzungen gespeichert und lassen sich mittels LockManager Software auslesen. So ist es auch ohne das Auslesen eines Schlossprotokolls möglich die Benutzung des MasterKeys anzuzeigen.

 **Hinweis: Die Programmierung der MasterKeys ist nur in Verbindung mit der LockManager Software möglich. Für Schlösser der Serien 500, 600 und 600 LEGIC ist ein LockManager ab Version 7 notwendig. Die anderen Serien können auch mit dem LockManager 6 genutzt werden.**

 **Hinweis: Jede Benutzung des MasterKeys wird im Schlossprotokoll gespeichert.**

5.3 MasterCode

Der MasterCode kann jederzeit zum Betätigen eines Schlosses oder zum Freigeben einer Sperre verwendet werden.

Der MasterCode ist mindestens 5-stellig und maximal 9-stellig. Darüber hinaus muss der MasterCode immer um mindestens Stelle länger sein, als der UserCode.

Der MasterCode eines Schlosses wird in den Applikationseinstellungen im LockManager hinterlegt. Dieser ist immer für eine Applikation (Teil der gesamten Anlage) gleich. Der MasterCode bleibt unverändert, bis die Schlossprogrammierung im LockManager geändert wird und die neue Programmierung in das Schloss eingespielt wird.

 **Hinweis: Jede Benutzung des MasterCodes wird im Schlossprotokoll gespeichert.**

5.3.1 MasterCode eingeben

Tasten       betätigen

 **Hinweis: 3 5 1 9 7 ist nur ein Beispielcode**

 **Hinweis: Die Bestätigung mit der Taste OK ist in einigen Betriebsarten nicht, oder nur beim Verschließen notwendig. In diesen Betriebsarten gibt das Schloss nach der Eingabe der letzten Ziffer die Betätigung frei.**

5.4 MasterCommand

Der MasterCommand kann jederzeit zum Betätigen eines Schlosses oder zum Freigeben einer Sperre verwendet werden.

Ein MasterCommand muss für seinen Einsatz in der LockManager Software vor der Benutzung erstellt und an die SAG Management App (SAM) übertragen werden. Folgende Parameter können eingestellt werden:

1. Schosnummer oder Schlossnummernbereich (örtliche Berechtigung)
2. Gültigkeit von, Gültigkeit bis (zeitliche Berechtigung)

So ist es möglich die MasterCommands nur für ein bestimmtes Schloss oder Schlossbereich und zusätzlich auch noch in einem bestimmten Zeitraum zu erzeugen.

In der SAG Management App (SAM) werden die letzten zehn Benutzungen von MasterCommands gespeichert und lassen sich anzeigen. So ist es auch ohne das Auslesen eines Schlossprotokolls möglich die Benutzung des MasterCommands anzuzeigen.

 **Hinweis: Die Programmierung der MasterCommands ist nur in Verbindung mit der LockManager Software (ab Version 7) möglich.**

 **Hinweis: Jede Benutzung des MasterCommands wird im Schlossprotokoll gespeichert.**

5.4.1 MasterCommand nutzen

Bluetooth wie im Kapitel 7.1.2 beschrieben aktivieren und auf die optische Rückmeldung (blau blinkende LED) warten. Anschließend den Anweisungen in der SAG Management App (SAM) folgen.

6 Datenstrukturen

Für die Datenstrukturen wird zwischen den Schlössern der Generation 1 (Serie 200, 300 und 400) sowie den Schlössern der Generation 2 (500, 600 und LEGIC) unterschieden. In der Generation 1 ist nur die Standard Datenstruktur (siehe Kapitel 6.2) verfügbar. Bei der Generation 2 werden abhängig von der Firmware-Version unterschiedliche Datenstrukturen unterstützt. Durch die Optimierung der Datenstrukturen und die Reduzierung auf die notwendigsten Daten wird eine optimale Geschwindigkeit in Abhängigkeit von der Anwendung garantiert. Durch die Auswahl der Datenstruktur entsteht im Gegenzug jedoch auch eine Funktionseinschränkung, die bei der Auswahl beachtet werden muss. Die verwendete Datenstruktur wird für Schlösser der Generation 2 im LockManager festgelegt und beim Programmieren der Schlösser übertragen.

6.1 Erläuterungen

Folgende Begrifflichkeiten werden zur Beschreibung der Datenstrukturen genutzt.

6.1.1 Applikation

Unter Applikation wird ein Schließbereich verstanden. Die Einteilung ist wichtig, da zum Beispiel in der Freien Schrankwahl die Anzahl der gleichzeitig nutzbaren Schränke in einem Bereich eingeschränkt werden kann.

Die Anzahl der Applikationen ist bei Schlössern der Generation 1 auf acht begrenzt. Bei Schlössern der Generation 2 gibt es lediglich Begrenzungen aufgrund des verfügbaren Speicherplatzes auf Transpondern. Wenden sie sich bei Fragen dazu an die SAG-Hotline.

6.1.2 Ausweisnummer

Die Ausweisnummer ist eine in der Anlage eindeutige Nummer des Schlüssels. Sie wird vom LockManager vergeben.

6.1.3 KGEN

Die KGEN (Key-Generation) ist die Generation des Schlüssels. Sie wird gemeinsam mit der Ausweisnummer im Schloss gespeichert. Das Schloss akzeptiert nur Transponder mit der KGEN gleich oder größer als die letzte gespeicherte KGEN. Andere Transponder werden abgelehnt. Das Update der KGEN erfolgt durch den Transponder mit der entsprechenden Ausweisnummer.

6.1.4 Gültigkeiten und Zeitpläne

Bitte beachten sie zu diesem Thema das Kapitel 7.4.

6.1.5 Sicherheitspin

Der Sicherheitspin ist eine Zwei-Faktor Authentifizierung. Der PIN muss am Schloss eingegeben werden, bevor der Transponder an das Schloss gehalten wird. Nur wenn der eingegebene PIN mit den Transponderdaten übereinstimmt und der Transponder grundsätzlich berechtigt ist, wird die Freigabe erteilt.

6.1.6 Berechtigung über Schließgruppen

Schließgruppen sind virtuelle Gruppen von Schlössern. Diese Gruppen können ein oder mehrere Schlösser enthalten. Jedes Schloss kann in der Generation 1 bis zu drei, in der Generation 2 bis zu fünf Gruppen zugeordnet sein. In einem Schlüssel wird gespeichert, an welchen Gruppen dieser berechtigt ist.

In jeder Applikation können maximal 500 Schließgruppen vergeben werden. Dabei ist es nicht relevant, ob in der Gruppe ein einzelnes oder mehrere Schlösser sind.

Die Berechtigungsart eignet sich besonders für Anlagen, die in einem Bereich nicht mehr als 500 Schlösser haben und bei denen ein Schlüssel viele Schlösser betätigen können muss. Ein Beispiel sind hier Türschließeanlagen in einem Industrieunternehmen.

6.1.7 Berechtigung über Schlossnummern

Schlossnummern sind eindeutige Nummern in einer Anlage. Es können bis zu 65.500 Schlossnummern vergeben werden. Jedes Schloss hat genau eine Schlossnummer.

Bei der Berechtigung über die Schlossnummer wird im Schlüssel die eindeutige Schlossnummer gespeichert.

Die Berechtigungsart eignet sich besonders für große Anlagen, in denen ein Schlüssel nur an wenigen Schlössern berechtigt ist. Ein Beispiel sind hier Umkleideanlagen in einem Industrieunternehmen.

6.1.8 Berechtigung über Bereiche

Bei der Berechtigung über Bereiche wird ein Schlossnummernbereich festgelegt, in dem der Schlüssel berechtigt ist. Der Bereich wird durch eine Start- und eine End-Schlossnummer festgelegt. So kann ein Schlüssel, der für den Bereich von 100 bis 110 berechtigt ist, zum Beispiel auch das Schloss 105 betätigen.

Die Berechtigungsart eignet sich besonders für Anlagen, in denen ein Mitarbeiter definierte Bereiche betreut. Ein Beispiel sind hier Reinigungskräfte in Hotels.

6.1.9 Blacklist

Über die Blacklist können KGEN / Ausweisnummer Kombinationen übertragen werden, die nicht mehr berechtigt sind. Die Blacklist ermöglicht es gesperrte KGENs über fremde Transponder in die Schlösser zu bringen, ohne mit der betroffenen Ausweisnummer an jedes Schloss gehen zu müssen.

6.1.10 Erlaubt mehrere Schlösser in freier Schrankwahl

Die Option, mehrere Schlösser in der freien Schrankwahl zu erlauben ist nur in Schlössern der Generation 2 mit einer entsprechenden Datenstruktur möglich. Die Option eignet sich zum Beispiel um in einem Schwimmbad Familientransponder zu erstellen, die mehrere Schlösser in der Umkleide belegen können. Ohne diese Option ist pro Applikation in der freien Schrankwahl immer nur ein Schloss verschließbar.



Hinweis: Durch den begrenzten Speicherplatz auf dem Transponder kann es vorkommen, dass nicht alle verschlossenen Schlösser auf dem Transponder gespeichert werden.

6.1.11 Nutzungsdauer und Aktion am Ende der Nutzungsdauer

Die Nutzungsdauer, sowie die Aktion am Ende der Nutzungsdauer können entweder im Schloss selber (für alle Nutzer gleich) oder auf dem Transponder (individuell je Nutzer) hinterlegt werden. Dabei gilt immer, dass die Daten auf dem Transponder priorisiert werden. Sie überschreiben also die Einstellungen im Schloss für diese Benutzung. Nur wenn auf dem Transponder keine Einstellungen hinterlegt sind, gelten die Einstellungen im Schloss. Für weitere Informationen beachten sie das Kapitel 7.2.

6.1.12 Datenspeicherung auf Transponder

Auf dem Transponder werden verschiedene Informationen, abhängig von der Datenstruktur, gespeichert. Die Daten können über den LockManager oder ein geeignetes Terminal ausgelesen werden. Alle Daten sind auf dem Transponder verschlüsselt.

Zu den gespeicherten Daten zählen die Schlossnummer von Schlössern, die mit diesem Transponder verschlossen worden sind sowie Batterieinformationen von den Schlössern.



Hinweis: Durch den begrenzten Speicherplatz auf dem Transponder kann es vorkommen, dass nicht alle verschlossenen Schlösser auf dem Transponder gespeichert werden. Darüber hinaus sind Batterieinformationen nur von der letzten Schließaktion vorhanden.

6.2 Standard Generation 1

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
1	1.0.0	mittel	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Ja
Gültigkeit (von - bis)	Ja
Sicherheitspin	Ja
Berechtigung über Schließgruppen	Ja
Berechtigung über Schlossnummern	Nein
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Nein
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Nein
Aktion am Ende der Nutzungsdauer	Nein
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Ja

Beschreibung:

Die Datenstruktur Standard Generation 1 ist die einzige Datenstruktur, die in den Schlössern der Serien 200, 300 und 400 unterstützt wird. Sie supportet alle notwendigen Daten für eine Feste Zuordnung, wie auch für eine Freie Schrankwahl und ist daher nicht für eine spezielle Anwendung optimiert.

Die Datenstruktur Standard Generation 1 arbeitet auf Sektor-Level eines MIFARE Classic Transponders. In dieser Datenstruktur kann in einem Sektor eine Applikationen untergebracht werden. Durch die Einschränkung des Speicherplatzes sind in einem MIFARE Classic Sektor lediglich 128 Schließgruppen möglich. Zusätzlich kann ein Extended Sektor genutzt werden, wodurch die Anzahl der Schließgruppen auf 500 steigt.

Bei anderen Transpondertechnologien werden alle 500 Schließgruppen in einem Speicherbereich abgelegt.

6.3 Standard Generation 2 - Allgemein

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	1.6.1	langsam	Obsolet - Datenstruktur wird ab Firmware-Version 2.9.1 nicht mehr unterstützt; Benötigt 2 Speicherbereiche

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Ja
Gültigkeit (von - bis)	Ja
Sicherheitspin	Ja
Berechtigung über Schließgruppen	Ja
Berechtigung über Schlossnummern	Ja
Berechtigung über Bereiche	Nein
Blacklist	Ja
Erlaubt mehrere Schlösser in freier Schrankwahl	Ja
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Ja
Aktion am Ende der Nutzungsdauer	Ja
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Ja

Beschreibung:

Die Datenstruktur Standard Generation 2 - Allgemein ist die einzige Datenstruktur, die in den Schlössern der Serien 500, 600 und LEGIC bis zur Firmware 2.9.1 unterstützt wird. Sie supportet alle notwendigen Daten für eine Feste Zuordnung, wie auch für eine Freie Schrankwahl und ist daher nicht für eine spezielle Anwendung optimiert. Durch die große Anwendungsvielfalt ist der Lese- und Schreibzugriff auf den Transponder langsam. Der Transponder muss daher lange in der korrekten Position (siehe Kapitel 1.2.3) gehalten werden.

In der Datenstruktur sind zwei Bereiche (Start- und Applikationsbereich) notwendig.

6.4 Freie Schrankwahl - Blocks

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	2.9.1	schnell	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Nein
Gültigkeit (von - bis)	Nein
Sicherheitspin	Nein
Berechtigung über Schließgruppen	Nein
Berechtigung über Schlossnummern	Nein
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Nein
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Nein
Aktion am Ende der Nutzungsdauer	Nein
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Ja

Beschreibung:

Die Datenstruktur Freie Schrankwahl - Blocks ist eine auf minimale Datenmengen ausgelegte Datenstruktur, die in den Schlössern der Serien 500, 600 und LEGIC ab der Firmware 2.9.1 unterstützt wird. Die Datenstruktur ist ausschließlich für die Freie Schrankwahl nutzbar und darauf ausgelegt, den Anwendungsfall schnellstmöglich zu verarbeiten. Hierzu sind die Lese- und Schreibzeiten minimiert.

Die Datenstruktur Freie Schrankwahl - Blocks arbeitet auf Block-Level eines MIFARE Classic Transponders. In dieser Datenstruktur können in einem Sektor zwei Applikationen untergebracht werden. Block 0 wird immer für allgemeine Daten genutzt, die für beide Applikationen identisch sind.

Bei anderen Transpondern gibt es keinen Mehrwert für die Datenstruktur im Vergleich zu Freie Schrankwahl - Minimal.

6.5 Freie Schrankwahl - Minimal

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	3.3.1	schnell	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Nein
Gültigkeit (von - bis)	Nein
Sicherheitspin	Nein
Berechtigung über Schließgruppen	Nein
Berechtigung über Schlossnummern	Nein
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Ja
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Nein
Aktion am Ende der Nutzungsdauer	Nein
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Ja

Beschreibung:

Die Datenstruktur Freie Schrankwahl - Minimal ist eine auf minimale Datenmengen ausgelegte Datenstruktur, die in den Schlössern der Serien 500, 600 und LEGIC ab der Firmware 3.3.1 unterstützt wird. Die Datenstruktur ist ausschließlich für die Freie Schrankwahl nutzbar und darauf ausgelegt, den Anwendungsfall schnellstmöglich zu verarbeiten. Hierzu sind die Lese- und Schreibzeiten minimiert.

Die Datenstruktur Freie Schrankwahl - Minimal arbeitet auf Sektor-Level eines MIFARE Classic Transponders. In dieser Datenstruktur kann in einem Sektor eine Applikationen untergebracht werden.

6.6 Freie Schrankwahl - Standard

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	3.4.1	mittel	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Nein
Gültigkeit (von - bis)	Ja
Sicherheitspin	Nein
Berechtigung über Schließgruppen	Nein
Berechtigung über Schlossnummern	Nein
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Ja
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Ja
Aktion am Ende der Nutzungsdauer	Ja
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Ja

Beschreibung:

Die Datenstruktur Freie Schrankwahl - Standard ist eine auf vollständige Funktionalität in der Freien Schrankwahl ausgelegte Datenstruktur. Sie wird in den Schlössern der Serien 500, 600 und LEGIC ab der Firmware 3.4.1 unterstützt. Die Datenstruktur ist ausschließlich für die Freie Schrankwahl nutzbar und darauf ausgelegt, den Anwendungsfall schnellstmöglich aber mit Zusatzfunktionen zu verarbeiten.

Die Datenstruktur Freie Schrankwahl - Standard arbeitet auf Sektor-Level eines MIFARE Classic Transponders. In dieser Datenstruktur kann in einem Sektor eine Applikationen untergebracht werden.

6.7 Feste Zuordnung - Schließgruppen

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	3.4.1	mittel	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Ja
Gültigkeit (von - bis)	Ja
Sicherheitspin	Nein
Berechtigung über Schließgruppen	Ja
Berechtigung über Schlossnummern	Nein
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Nein
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Nein
Aktion am Ende der Nutzungsdauer	Nein
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Nein

Beschreibung:

Die Datenstruktur Feste Zuordnung - Schließgruppen ist eine auf die feste Zuordnung ausgelegte Datenstruktur, die in den Schlössern der Serien 500, 600 und LEGIC ab der Firmware 3.4.1 unterstützt wird. Die Datenstruktur ist ausschließlich für die feste Zuordnung nutzbar und darauf ausgelegt.

Die Datenstruktur Feste Zuordnung - Schließgruppen arbeitet auf Sektor-Level eines MIFARE Classic Transponders. In dieser Datenstruktur kann in einem Sektor eine Applikation untergebracht werden. Durch die Einschränkung des Speicherplatzes sind in einem MIFARE Classic Sektor lediglich 128 Schließgruppen möglich. Zusätzlich kann ein Extended Sektor genutzt werden, wodurch die Anzahl der Schließgruppen auf 500 steigt.

Bei anderen Transpondertechnologien werden alle 500 Schließgruppen in einem Speicherbereich abgelegt.

6.8 Feste Zuordnung - Industrie

Schloss Generation	Min. Firmware	Geschwindigkeit	Bemerkung
2	3.4.1	mittel	

Funktion	Support
Ausweisnummer	Ja
KGEN	Ja
Zeitpläne	Ja
Gültigkeit (von - bis)	Ja
Sicherheitspin	Nein
Berechtigung über Schließgruppen	Nein
Berechtigung über Schlossnummern	Ja
Berechtigung über Bereiche	Nein
Blacklist	Nein
Erlaubt mehrere Schlösser in freier Schrankwahl	Nein
Nutzungsdauer (Zeitspanne oder Zeitpunkt)	Nein
Aktion am Ende der Nutzungsdauer	Nein
Speicherung Batteriezustand Schloss	Ja
Speicherung verschlossener Schlösser	Nein

Beschreibung:

Die Datenstruktur Feste Zuordnung - Industrie ist eine auf die feste Zuordnung von wenigen Schlössern in einer großen Anlage ausgelegte Datenstruktur, die in den Schlössern der Serien 500, 600 und LEGIC ab der Firmware 3.4.1 unterstützt wird.

Die Datenstruktur Feste Zuordnung - Industrie arbeitet auf Sektor-Level eines MIFARE Classic Transponders. In dieser Datenstruktur kann in einem Sektor eine Applikationen untergebracht werden. Bei der Datenstruktur wird die Zuordnung auf dem Transponder über die Schlossnummer durchgeführt.

Durch die Einschränkung des Speicherplatzes sind in einem MIFARE Classic Sektor lediglich 8 Schlossnummern möglich. Zusätzlich kann ein Extended Sektor genutzt werden, wodurch die Anzahl der speicherbaren Schlossnummern auf 32 Stück steigt.

Bei anderen Transpondertechnologien werden alle 32 Schlossnummern in einem Speicherbereich abgelegt.

7 Funktionen

Im folgenden Kapitel sind einige Funktionen des Schlosses und ihre Eigenheiten näher beschrieben.

7.1 PIN-Codes

PIN-Codes können am Schloss über die kapazitive Tastatur eingegeben werden. Die Nutzung von PIN-Codes ist in der freien (beliebiger PIN-Code mit der eingestellten Länge) oder in der festen (PIN-Code ist im Schloss gespeichert) Zuordnung möglich. In allen Betriebsarten müssen die folgenden Hinweise beachtet werden.

 **Hinweis: Die Eingabe von PIN-Codes darf nicht länger als 30 Sekunden dauern. Anschließend wird die bisherige Eingabe verworfen.**

In einer Festen Zuordnung müssen die PIN-Codes ins Schloss einprogrammiert werden. Dabei können bei Schlössern der Generation 1 bis zu 100 und bei Schlössern der Generation 2 bis zu 400 PIN-Codes gespeichert werden. Feste PIN-Codes unterstützen Gültigkeiten und Zeitpläne.

7.1.1 Sperre durch Falscheingaben

Wurde vier-Mal ein nicht berechtigter PIN-Code (z.B. anderer Code wie zum Verschließen) eingegeben, sperrt sich das Schloss für 60 Sekunden. In dieser Zeit werden keine PIN-Codes akzeptiert, selbst wenn der dann eingegebene Code berechtigt ist. Eine Ausnahme bildet hier ausschließlich der MasterCode. Nach 20 nicht berechtigten Eingaben sperrt sich das Schloss dauerhaft. Es wird anschließend nur noch der MasterCode akzeptiert. Die Eingabe des MasterCodes setzt die Sperre zurück und das Schloss kann wieder normal genutzt werden.

 **Hinweis: Die Sperren sollen das Erraten von PIN-Codes durch ausprobieren verhindern.
Eine Minute Sperre nach vier nicht berechtigten Eingaben
Dauerhafte Sperre nach 20 nicht berechtigten Eingaben**

7.1.2 Aktivieren von Bluetooth

Bei Schlössern der Serie 500 ist Bluetooth über den PIN-Code     aktivierbar. Bei anderen Schlössern der Generation 2 erfolgt die Aktivierung von Bluetooth ausschließlich über einen entsprechenden Systemtransponder.

7.2 Automatische Aktionen

Automatische Aktionen werden nach einer definierten Dauer oder zu einem definierten Zeitpunkt ausgeführt. Dauer, Zeitpunkt und die Art der Aktion können dabei entweder fest in das Schloss einprogrammiert (über den LockManager) oder pro Transponder individuell festgelegt werden. Die Einstellung auf dem Transponder wird gegenüber der Schlosseinstellung immer priorisiert.

7.2.1 Dauer

Die Dauer wird in Stunden und Minuten angegeben. Sie wird ab dem Zeitpunkt des letzten Verschließens gerechnet. Wird also ein Schloss mit einer Dauer von 2 Stunden um 14:35 verschlossen, endet die Dauer um 16:35.

7.2.2 Zeitpunkt

Der Zeitpunkt ist eine absolute Angabe. Eine Aktion wird immer dann ausgeführt, wenn der einprogrammierte Zeitpunkt (z.B. 01:00) erreicht wird.



Hinweis: Bei der Verwendung von Zeitpunkten muss darauf geachtet werden, dass die Uhrzeit im Schloss korrekt ist. Eine falsche Uhrzeit kann zu ungewollten Aktionen auch im laufenden Betrieb führen.

Bei Anlagen der Generation 2, die CLW verwenden ist darauf zu achten, dass die Uhrzeit im Gateway korrekt ist (NTP-Server gemäß RFC 5905 (NTPv4)). Näheres hierzu ist in der CLW-Dokumentation zu finden.

7.2.3 Öffnen

Ist als Aktion am Nutzungsende „Öffnen“ eingestellt, so öffnet sich das Schloss automatisch. Entweder zu einem festgelegten Zeitpunkt, oder nach einer definierten Dauer der Benutzung.

7.2.4 Sperren

Ist als Aktion am Nutzungsende „Sperren“ eingestellt, so sperrt sich das Schloss automatisch. Entweder zu einem festgelegten Zeitpunkt, oder nach einer definierten Dauer der Benutzung.

Ein gesperrtes Schloss kann von einem berechtigten PIN-Code oder Transponder nicht mehr geöffnet werden. Lediglich ein MasterKey / MasterCode kann das Schloss öffnen und gleichzeitig auch entsperren.

7.3 Zeitzone

Über die Einstellung der Zeitzone wird festgelegt, in welcher globalen Zeitzone sich das Schloss befindet. Die Einstellung wird unter anderem dazu verwendet, die Sommer-/Winterzeit Umstellung richtig durchzuführen. Daher ist auf die Einstellung bei der Inbetriebnahme der Anlage zu achten.

 **Hinweis:** Die Einstellung ist nur bei Schlössern der Generation 2 verfügbar. Schlösser der Generation 1 verwenden immer die Einstellungen der Zeitzone Mitteleuropäische Normalzeit.

7.4 Zeitfunktionen

Schlösser der Serie *SAFE-O-TRONIC access*[®] LSW sind mit einer Echtzeituhr ausgestattet, die eine Vielzahl an Benutzerfunktionen zur Verfügung stellt. Als Grundfunktionen stehen die unten aufgeführten Zeitlimits zur Verfügung. Zusätzlich können weitere Zeitlimitierungen genutzt werden. Außerhalb der Zeitlimits wird die Betätigung des Schlosses unterbunden und das Schloss gibt nicht frei. Alle Zeitfunktionen sind bei allen UserDaten (PIN, RFID und BLE) möglich. Bei RFID und BLE Daten können die Beschränkungen auf den entsprechenden Medien (RFID-Datenträger oder BLE-Daten) hinterlegt werden. Bei PIN Codes müssen die Beschränkungen ins Schloss programmiert werden.

 **Hinweis:** Bei der Verwendung von Zeitfunktionen muss darauf geachtet werden, dass die Uhrzeit im Schloss korrekt ist. Eine falsche Uhrzeit kann zu ungewollten Aktionen oder Ablehnungen auch im laufenden Betrieb führen.

Bei Anlagen der Generation 2, die CLW verwenden ist darauf zu achten, dass die Uhrzeit im Gateway korrekt ist (NTP-Server gemäß RFC 5905 (NTPv4)). Näheres hierzu ist in der CLW-Dokumentation zu finden.

7.4.1 Gültig ab / bis / von-bis

Bei diesen Zeitlimits wird festgelegt, ab wann, bis wann oder in welchem Zeitraum die UserDaten gültig sind. Die Einschränkungen können jeweils für einen Zeitpunkt (Datum und Uhrzeit) gemacht werden. Bei der Beschränkung für einen Zeitraum müssen zwei Zeitpunkte (jeweils Datum und Uhrzeit) angegeben werden.

7.4.2 Zeitpläne - Standard

Zusätzlich können 8 wochentags bezogene Zeitpläne im Schloss programmiert werden. Damit kann die Gültigkeit UserDaten auf bis zu 8 unterschiedliche Zeiträume eingeschränkt werden (z.B. jeweils Montags und Mittwochs zwischen 8:30 Uhr Und 16:20). Es können max. 8 Zeitpläne in jedem Schloss hinterlegt werden. Im LockManager wird festgelegt welche Zeitpläne im Schloss aktiv sind und wie der einzelne Zeitplan definiert ist. Jeder Zeitplan enthält folgende Werte:

- Gültigkeitsbeginn – Minute, Stunde
- Gültigkeitsende – Minute, Stunde
- Gültige Wochentage – Mo, Di, Mi, Do, Fr, Sa, So, Feiertag

Ein Zeitplan im Schloss ist nur gültig, wenn diese aktiviert wurde. Wird ein Zeitplan ausgewählt, der nicht aktiv ist, so sind die UserDaten ohne Einschränkung gültig.

 **Hinweis:** Zeitpläne können nur mit UserKeys (RFID) oder UserCommands (BLE) verwendet werden. Die Verwendung mit UserCodes (PIN) oder TGC Codes ist nicht möglich.

 **Hinweis:** Zeitpläne können bei Schlössern der Generation 2 auch für Nachtschichten genutzt werden. Dabei beginnt der Zeitplan an den ausgewählten Tagen zur eingegebenen Uhrzeit und endet an der eingegebenen Uhrzeit des Folgetages.

 **Hinweis:** Bei der Nutzung von Zeitplänen kann ein Schloss auch außerhalb eines gültigen Zeitplans immer geöffnet werden. Ein Verschließen ist nicht möglich.

7.4.3 Zeitpläne - Nutzungszeiten

Einzelne Zeitpläne können für andere Funktionen genutzt werden. Eine solche Funktion ist die Nutzungszeit. Diese wird im Schloss hinterlegt und unabhängig für alle User-Eingaben am Schloss geprüft. Nur Eingaben, die innerhalb der angegebenen Zeiten stattfinden, werden weiter verarbeitet und führen bei entsprechender Berechtigung zu einer Schlossbetätigung.

Ist die Option "Öffnen außerhalb der Nutzungszeit erlauben" im LockManager für die Applikation nicht aktiviert, so kann ein verschlossenes Schloss nach Ende der Nutzungszeit nur über MasterKey oder MasterCode geöffnet werden. Mit aktiver Option kann der User das Schloss auch außerhalb der Nutzungszeit noch öffnen.

7.4.4 Schedules - Usage times

Individual schedules can be used for other functions. One such function is the usage time. This is stored in the lock and checked independently for all user entries on the lock. Only entries that take place within the specified times are processed further and, if the appropriate authorization is given, result in the lock being activated.

If the "Allow opening outside of usage time" option is not activated in the LockManager for the application, a locked lock can only be opened with a MasterKey or MasterCode after the end of the usage time. With this option activated, the user can still open the lock outside of the usage time.

8 Allgemeine Informationen

8.1 LED-Anzeige

Alle wichtigen Aktionen und Betriebszustände werden durch die LED Anzeige signalisiert und sollen dazu beitragen, bei Störungen und Fehlbedienungen die Ursachen zu finden. Die Bedeutung der einzelnen Signale ist in folgenden Kapiteln aufgeführt.



Hinweis:

-  bedeutet, dass die entsprechend farbige LED blinkt.
-  bedeutet, dass die entsprechend farbige LED für die angegebene Dauer aktiv ist.

8.1.1 LED-Anzeige Serie 200, 300 und 400



Abbildung 8.1 – Position der verschiedenen LEDs

Tabelle 8.1 – Übersicht über die verschiedenen LED Statusmeldungen

grün	rot	grün	rot	Anzeige	Aktion
				Schnell	Programmiermodus
				Alle 3 Sekunden	Die Sperrzeit ist aktiv Es wurde viermal ein falscher Code eingegeben
				1 Sekunde	Tasteneingabe
				1 Sekunde	Abbruch Taste (X) betätigt

grün	rot	grün	rot	Anzeige	Aktion
				3 mal	Falsche Handhabung - Drehknopf wurde nicht betätigt
				Abwechselnd	Betätigung möglich
				1 Sekunde	Verriegeln / Programmierung erfolgreich
				2 Sekunde	Entriegeln erfolgreich
				0,5 Sekunden	Code wurde akzeptiert
				3 Sekunden	Interne Funktionsstörung
				erst rot dann grün	Die durch MasterKey 1 ausgelöste Sperre wurde aufgehoben
				3 mal schnell	Codeeingabe verweigert - Sperre durch MasterKey 1
				3 mal	Batterie Warnung
				5 mal	Batterie leer
				3 mal	Reset durchgeführt

8.1.2 LED-Anzeige Serie 500, 600 und 600 LEGIC



Abbildung 8.2 – Position der verschiedenen LEDs

Statusmeldungen Version 1.x

Tabelle 8.3 – Übersicht über die verschiedenen LED Statusmeldungen

blau	rot	oran- ge	grün	Anzeige	Aktion
				3 mal	Reset durchgeführt
				Dauerhaft	Initialisierung des Speichers
				1 mal	Tasteneingabe
				8 mal	PIN akzeptiert
				1 mal	Abbruch Taste betätigt (X)
				1 mal	Abbruch der Eingabe
				Dauerhaft	RFID Verarbeitung
				1 Sekunde	Programmierung erfolgreich
					Reset in Arbeit

blau	rot	oran- ge	grün	Anzeige	Aktion
				6 mal	Batterie Warnung
				10 mal	Batterie leer
				alle 500ms	Betätigung möglich
				4 mal	Falsche Handhabung - Drehknopf wurde nicht betätigt
				500ms	Verriegeln / Entriegeln erfolgreich
				alle 10s	Sperrzeit aktiv (eine Minute)
				jede Sekunde	Bluetooth aktiv
				1 mal	Bluetooth Verbindung hergestellt
				1 mal	Bluetooth Daten abgelehnt
				1 mal	Bluetooth beendet
				1,5 Sekunden	Interne Funktionsstörung
				1 Sekunde	FW Update erwartet
				Dauerhaft	Werksreset des Speichers

Statusmeldungen Version 2.x sowie 3.1.x

Tabelle 8.5 – Übersicht über die verschiedenen LED Statusmeldungen

blau	rot	oran- ge	grün	Anzeige	Aktion
				1 Sekunde	Power On
				Dauerhaft	Initialisierung des Speichers
				5 Sekunden	Einstellungen wiederherstellen
				Dauerhaft	RFID Verarbeitung
				Abwechselnd alle 50ms	Motorfahrt
				Abwechselnd je 100ms (max. 2 Sekunden)	Batterie-Warnung
				Abwechselnd je 100ms (max. 2 Sekunden)	Batterie leer
				Abwechselnd je 50ms (max. 2 Sekunden)	Motorfehler
				Max. 30 Sekunden	Betätigung erfolgreich (oder RFID entfernt)
				Max. 30 Sekunden	Abgelehnt (oder RFID entfernt)
				24ms	Bluetooth aktiv
				1 Sekunde	Programmierung erfolgreich

blau	rot	oran- ge	grün	Anzeige	Aktion
				200ms	Bluetooth Daten abgelehnt
				Alle 3 Sekunden (10ms)	Schloss verschossen
				Alle 3 Sekunden (10ms)	Schloss gesperrt (MasterKey notwendig)

Statusmeldungen ab Version 3.2.x

Tabelle 8.7 – Übersicht über die verschiedenen LED Statusmeldungen

blau	rot	oran- ge	grün	Anzeige	Aktion
				Links nach rechts	Power On
				Abwechselnd je 200ms	Speicherinitialisierung
				Blinken alle 200 ms	Interne Funktionsstörung
				Blinken alle 200 ms	Schwerwiegende Funktionsstörung - Kontaktieren sie die Hotline
				Blinken	Schloss dauerhaft blockiert - Kontaktieren sie die Hotline
				Blinken alle 200ms	BLE aktiv - Verbindung möglich
				Blinken alle 200ms	BLE Verbindung hergestellt
				Blinken alle 200ms	BLE deaktiviert - keine Verbindung mehr möglich
				Blinkt 2 mal	BLE Daten abgelehnt / ungültig
				1 Sekunde	BLE Daten erfolgreich übertragen und akzeptiert
				Blinken alle 200 ms	Reset des Schlosses wird durchgeführt

blau	rot	oran- ge	grün	Anzeige	Aktion
				Blinken alle 200 ms	Werksreset des Schlosses wird durchgeführt
				Blinken alle 200 ms	Update der Firmware erwartet
				200ms leuchten	Tasteneingabe
				2 mal Blinken	Abbruch der Eingabe
				3 mal Blinken	RFID Daten wurden abgelehnt
				Blinken alle 200 ms	RFID aktiv und Transponder wird verarbeitet
				600ms	Daten akzeptiert
				2 mal Blinken	Batteriewarnung - Austausch der Batterie empfohlen
				3 mal Blinken	Batteriealarm - Austausch der Batterie notwendig
				Blinken alle 200 ms	Betätigung des Schlosses möglich
				Blinken alle 200 ms	Verriegeln erfolgreich

blau	rot	oran- ge	grün	Anzeige	Aktion
				Blinken alle 200 ms	Entriegeln erfolgreich
				Blinken alle 200 ms	Falsche Handhabung des Schlosses - Knopf wurde nicht gedreht
				Blinken alle 5 Sekunden	Schloss verschlossen
				Blinken alle 200 ms	Schloss für die Benutzung gesperrt - Zu viele falsche PINs eingegeben

8.2 Fehlerbehebung

Aus den Statusmeldungen der LED Anzeige können Sie Fehler und die Fehlbedienungen entnehmen und dann entsprechend beseitigen. Sollten andere, nicht definierte Zustände auftreten und das Schloss funktioniert trotz ausgetauschter Batterie und durchgeführtem Reset mittels ResetBefehl und Neuprogrammierung nicht einwandfrei, wenden Sie sich an den Support.

8.3 Batterieüberwachung

Die automatische Batterieüberwachung von *SAFE-O-TRONIC access[®]* stellt sicher, dass ein Schloss mit zu geringer Batteriespannung nicht mehr verriegelt werden kann. Hierzu gibt es eine Vorwarnung durch die LED's. Ein Batteriewechsel ist dann kurzfristig empfehlenswert. Die genaue Signalisierung ist dem Kapitel 8.1 zu entnehmen

Wird kein Batteriewechsel vorgenommen, erfolgt nach einiger Zeit ein Alarm. Dies wird anders durch die LED's signalisiert. Jetzt muss ein Batteriewechsel vorgenommen werden. In diesem Zustand kann das Schloss nur noch geöffnet, aber nicht mehr verschlossen werden.

Die Schlösser dürfen ausschließlich mit, von der Schulte-Schlagbaum AG, zugelassenen Batterien betrieben werden. Der Einsatz nicht zugelassener Batterien kann zu Fehlfunktionen und zur Beschädigung des Schlosses führen.

8.3.1 Batteriewechsel

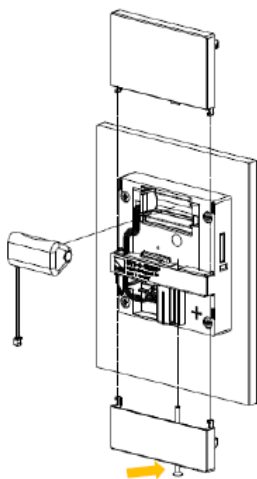


Abbildung 8.3 – Austausch der Batterie

1. Schraube TX20 an der Unterseite der Inneneinheit lösen.
2. Unteren und oberen Deckel der Inneneinheit abnehmen.
3. Die zweipolige Steckverbindung des Batteriepacks trennen. Dabei muss der Stecker grade herausgezogen werden, da ansonsten die Anschlussdose beschädigt werden kann.
4. Alte Batterie entfernen.
5. Neue Batterie einsetzen und Kabel durch das Loch auf der linken Seite der Inneneinheit führen.
6. Neues Batteriepack mit Steckverbindung verbinden.
7. Deckel einsetzen und wieder zuschrauben.

⚠ Hinweis: Die Schraube des Batteriefachs darf maximal handfest angezogen werden. Es darf zu keiner Verformung der oberen Abdeckung kommen.

⚠ Hinweis: Bei einem Batteriewechsel wird kein Code gelöscht. Sicherheitshalber sollte nach einem Batteriewechsel die Uhrzeit neu gestellt werden.

⚠ Hinweis: Das leere Batteriepack ist gemäß der geltenden Umweltbestimmungen fachgerecht zu entsorgen!

8.4 Austausch der Nummernplatte

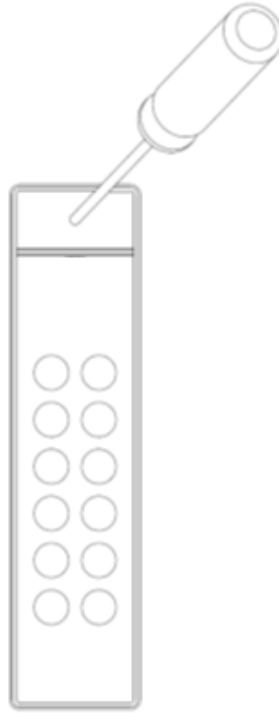


Abbildung 8.4 – Austausch der Nummernplatte

Die alte Nummernplatte wird nach Einstechen mit einem kleinen Schraubendreher in der Mitte der Nummernplatte aus dem LSW herausgehoben. Danach kann eine neue Nummernplatte eingeklipst werden.

⚠ Hinweis: Beim Austausch wird die alte Nummernplatte zerstört.

8.5 Wartung und Pflege

SAFE-O-TRONIC access[®] LSW Schlösser sind wartungsfrei. Die Schlösser dürfen auf keinen Fall mit mineralölhaltigen Schmiermitteln geölt oder gefettet werden. Die Reinigung darf nur mit nicht klebenden, rückstandsfreien Reinigungs- und Desinfektionsmitteln erfolgen. Für die Pflege dürfen keine scharfen Reinigungsmittel, Säuren oder Laugen eingesetzt werden. Ebenso darf kein Druckreiniger eingesetzt werden. Auch das Abspritzen der Schlösser, z.B. mittels Schlauch ist nicht zulässig und kann zu einer Zerstörung und Haftungsausschluss führen.

8.6 Update der Firmware

Ein Update der Firmware wird, sofern es verfügbar ist, durch SAG zur Verfügung gestellt. Updates enthalten in der Regel Funktionserweiterungen, Fehlerbehebungen oder Sicherheitsupdates. Für die Durch-

führung von Updates wird zwischen den Schlössern der Generation 1 (Serie 200, 300 und 400) sowie den Schlössern der Generation 2 (500, 600 und LEGIC) unterschieden. Alle Updates werden einzeln an den Schlössern durchgeführt.

 **Hinweis: Updates müssen immer durch SAG oder zumindest unter Anleitung von SAG durchgeführt werden.**

8.6.1 Update bei Schlössern der Generation 1

Schlösser der Generation 1 werden über einen entsprechend vorbereiteten Communicator (Hardware, welche von SAG zur Verfügung gestellt wird) über die RFID-Schnittstelle mit einem Update bespielt. Das Schloss muss sich dazu im programmierten Zustand befinden und der Communicator muss für die entsprechende Anlage konfiguriert sein. Um das Update zu starten, wird der Communicator wie ein RFID-Transponder (Hinweise aus Kapitel ?? beachten) an das Schloss gehalten. Die grüne LED blinkt solange die Übertragung andauert.

 **Hinweis: Während der Übertragung darf der Communicator nicht vom Schloss entfernt werden. Der Abstand darf maximal 1cm betragen.**

Das Schloss bestätigt die Übertragung und das Firmware-Update nach erfolgreicher Durchführung über die LEDs.

8.6.2 Update bei Schlössern der Generation 2

Schlösser der Generation 2 werden über Bluetooth mit einer neuen Firmware bespielt. Dazu muss das Schloss zunächst mit einem speziellen Bluetooth-Befehl aus der SAG Management App (SAM) heraus in den Update-Modus gebracht werden. Bei programmierten Schlössern muss der Befehl zur Anlage passen. Anschließend wird über eine zweite App das Update übertragen.

Zur Durchführung eines Firmware-Updates beachten sie bitte das separate Handbuch „Firmware-Update über Bluetooth“ welches sie über die SAG-Hotline in der jeweils aktuellen Fassung erhalten können.

9 Technische Daten

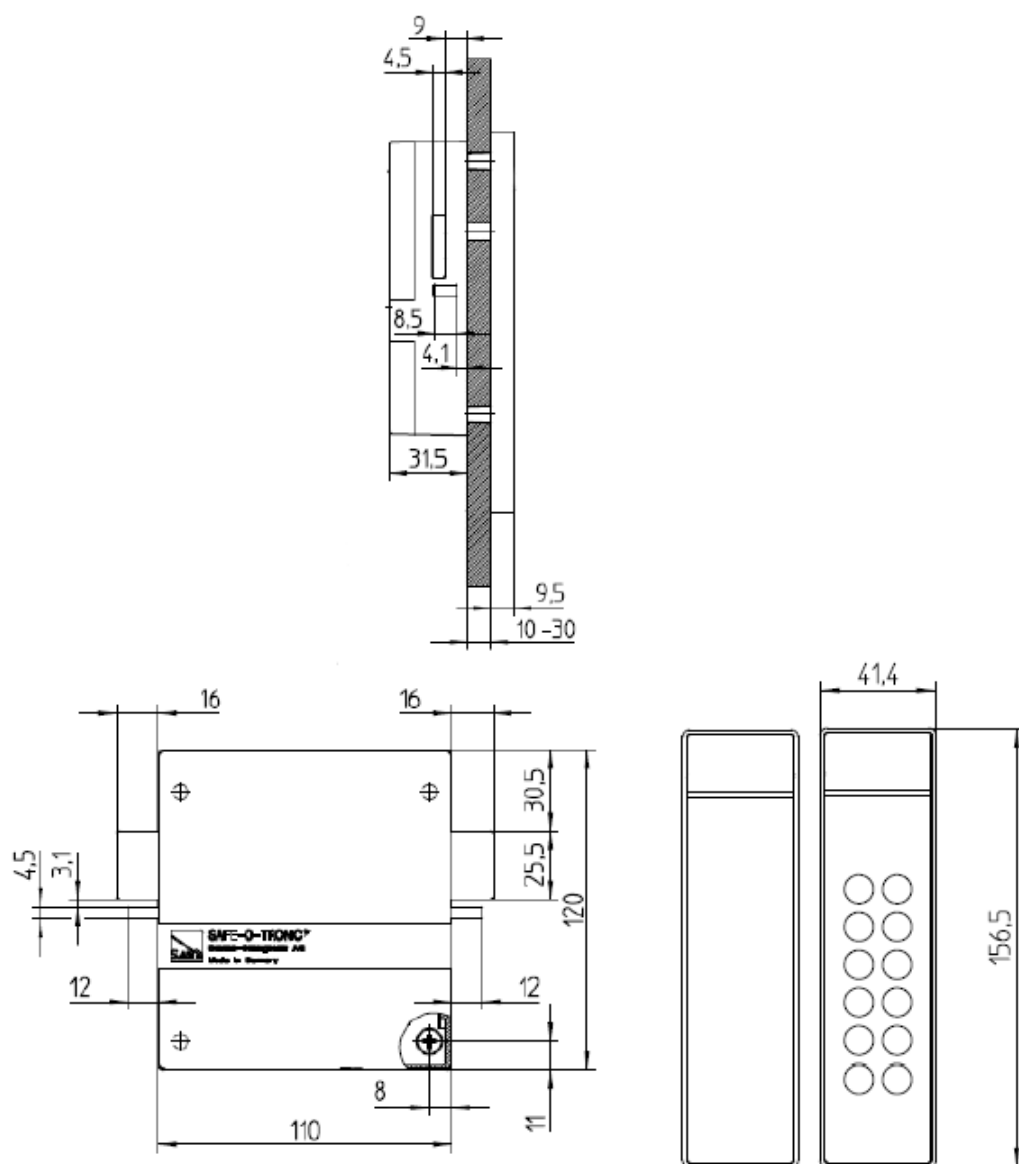


Abbildung 9.1 – Technische Abmaße - Oben: Seitenansicht mit Türe (grau), Außeneinheit (rechts) und Inneneinheit (links) - Unten: Inneneinheit (links) und Außeneinheit (rechts)

Tabelle 9.1 – Technische Daten

Anzeige Elemente Serie 200, 300, 400	2 x LED grün; 2 x LED rot
Anzeige Elemente Serie 500, 600, 600 LEGIC	1 x LED grün; 1 x LED gelb; 1 x LED rot; 1 x LED blau
Akustische Meldung	Signalgeber
Batterie	Batteriepack: 3 x Alkali-Zellen (AA)
Batterielebensdauer* für Serie 300	ca. 4 Jahre oder 55.000 Betätigungen
Temperaturbereich Funktion	0 bis +55°C
Temperaturbereich Lagerung	-15 bis +55°C
Relative Luftfeuchte	10 - 90 % nicht kondensierend
Schutzart Außeneinheit	IP 65 (Hinweis beachten)
Schutzart Inneneinheit	für den geschützten Innenbereich
RFID Frequenz	13,56MHz
RFID Sendeleistung	-11dBm
BLE Frequenz (ab Serie 500)	2,4GHz
BLE Sendeleistung (ab Serie 500)	+3dBm
Gewicht	ca. 300g
Gehäuseabmaße Außengehäuse (H x B x T)	156,5mm x 41,4mm x 9,5mm
Gehäuseabmaße Innengehäuse (H x B x T)	120mm x 110mm x 31,5mm
Farbe Gehäuse	ähnlich RAL 9006 (weißaluminium)
Farbe Blende	schwarz oder weiß
Türstärke	1 bis 30mm



Hinweis: Bitte beachten sie die Hinweise zur Batterielebensdauer im Kapitel 10.



Hinweis: Bitte beachten sie dass die Schutzart für die Außeneinheit nur bei korrekter Montage gegeben ist. Bei Verwendung einer Adaptionkonstruktion (z.B. für Glastüren) ist die Schutzart nicht mehr gegeben. Diese sind dann nur für den geschützten Innenbereich einsetzbar.

10 Technische Hinweise zu den Batterien und Batteriepacks

In diesem Kapitel werden wichtige Hinweise zur Batterielebensdauer und den verwendeten Batterien in *SAFE-O-TRONIC access*[®] Schließsystemen gegeben.

Die folgenden Temperaturbereiche gelten für alle Schließsysteme:

Lagerung: -15 bis +55°C

Funktion Alkali Batterien: 0 bis +55°C

Funktion Lithium Batterien: 0 bis +55°C

Temperaturen unterhalb von 0°C führen zu einer eingeschränkten Lebensdauer der Batterien.

10.1 Baureihen und Batterielebensdauer

Die folgenden Batterien oder Batteriepacks kommen in den *SAFE-O-TRONIC access*[®] Schließsystemen zum Einsatz.

 **Hinweis:** Bei der angegebenen Batterielebensdauer sind immer die im Kapitel 10.2 aufgeführten Hinweise und Einschränkungen zu beachten.

 **Hinweis:** Die angegebene Batterielebensdauer gilt jeweils für die Schließsystemvariante 300

10.1.1 LS

Standard Batteriepack: Alkali-Mangan 3xLR03 (AAA)

Artikelnummer: # 38400200

Batterielebensdauer* ca. 3 Jahre oder ca. 30.000 Betätigungen

Sonder-Batteriepack: Lithium 3xLR03 (AAA)

Artikelnummer: # 38400200L

Batterielebensdauer* ca. 5 Jahre oder ca. 50.000 Betätigungen

10.1.2 LSW

Standard Batteriepack: Alkali-Mangan 3xLR06 (AA)

Artikelnummer: # 38450901

Batterielebensdauer* offline ca. 4 Jahre oder ca. 55.000 Betätigungen

Batterielebensdauer* online (Funk - Status) ca. 3 Jahre oder ca. 30.000 Betätigungen

Batteriehalter: für 3xLR03 (AA)

Artikelnummer: # 38450902

Die Batterien zum Batteriehalter müssen bauseitig gestellt werden. Somit können keine Aussagen zur Batterielebensdauer getroffen werden. Batterieempfehlung: Alkali-Mangan, Panasonic Powerline

10.1.3 DS

Standard Batteriepack: Alkali-Mangan 3xLR03 (AAA)

Artikelnummer: # 38400200

Batterielebensdauer* ca. 3 Jahre oder ca. 30.000 Betätigungen

Sonder-Batteriepack: Lithium 3xLR03 (AAA)

Artikelnummer: # 38400200L

Batterielebensdauer* ca. 5 Jahre oder ca. 50.000 Betätigungen

10.1.4 CS

Standard Batterie: 2x Lithium-Mangandioxid CR-2L (3V)

Artikelnummer: # 50203EK-B

Batterielebensdauer* ca. 3 Jahre oder ca. 30.000 Betätigungen

10.1.5 DSH

Standard Batterie: 1x Lithium-Mangandioxid CR-2L (3V)

Artikelnummer: # 50203EK-B

Batterielebensdauer* ca. 2 Jahre oder ca. 20.000 Betätigungen

10.2 Allgemeine Hinweise zur Batterielebensdauer

Die Batterielebensdauer wurde unter praxisnahen Laborbedingungen ermittelt. Somit sind positive oder negative Abweichungen von diesen Angaben in der Praxisanwendung durchaus gegeben. In der folgenden Aufstellung werden einige Eigenschaften und Maßnahmen aufgelistet, welche die genannte Batterielebensdauer beeinflussen können.

10.2.1 Schließsystemvariante

Die einzelnen Schließsysteme der Baureihe *SAFE-O-TRONIC access*[®] unterscheiden sich in ihrer Funktionalität und Ausstattung. Es gibt Schließsysteme mit PIN Funktionalität (101 und 200), mit RFID Funktionalität (300), mit einer Kombination PIN und RFID Funktionalität (400), mit einer Kombination PIN und BLE Funktionalität (500) und mit einer Kombination aus PIN, BLE und RFID Funktionalität (600). Der Energiebedarf ist bei diesen Schließsystemen unterschiedlich und beeinflusst auch die Batterielebensdauer. So ist z.B. der Energiebedarf bei einer 400er und 500er Ausführung ca. 1,4 x höher als bei der 300er Ausführung. Die angegebene Batterielebensdauer bezieht sich auf einen mittleren Wert, der mit der 300er Ausführung ermittelt wurde.

10.2.2 Transponder

Der Energiebedarf der Schließsysteme ist von dem verwendeten Transpondertyp abhängig. So benötigt der DesFire Transponder in der Transponderfamilie Mifare die meiste Energie bei einem Lese- oder Schreibzugriff.

10.2.3 Konfiguration und Nutzerverhalten

Die Konfiguration (Freigabezeit, Statusanzeige, usw.) und das Nutzerverhalten beeinflussen die Batterielebensdauer des Schließsystems. Einzelheiten hierzu finden sie in den entsprechenden Kapiteln der Handbücher.

10.2.4 Hinweise zum Batteriewechsel

- Der Zeitpunkt, wann das Batteriepack *SAFE-O-TRONIC access*[®] ersetzt werden muss, hängt davon ab, wie oft das Schließsystem betätigt wurde, oder wie lange das Batteriepack eingebaut ist und von der Umgebungstemperatur, in der das Schließsystem betrieben wird.
- Auf Grund der geringen, aber unvermeidlichen Selbstentladung der Batterien kann es notwendig werden, das Batteriepack vor Erreichen der angegebenen Betätigungsanzahl zu tauschen.
- Es besteht Verletzungsgefahr durch unsachgemäße Handhabung der Batterien.
- Einen Batteriewechsel nur bei geöffneter Tür durchführen. Eine Funktionskontrolle nach einem Batteriewechsel sollte immer bei geöffneter Tür durchgeführt werden.
- Einbau und Batteriewechsel nur durch geschultes Fachpersonal gemäß dieser Bedienungs- und Montageanleitung durchführen lassen.
- Nach jedem Batteriewechsel die Uhrzeit überprüfen, muss gegebenenfalls die aktuelle Uhrzeit neu programmiert werden.
- Nur von Schulte-Schlagbaum bezogene Batteriepacks verwenden.
- Batterie nicht über die angegebene Lagertemperatur erhitzen.
- Batteriewechsel CS300: Beschädigung des Dichtungsringes durch unsachgemäßen Umgang vermeiden. Keine spitzen Gegenstände benutzen und den Dichtungsring nicht stärker dehnen als zum Aufschieben erforderlich.
- Beim Einsetzen der Batterien auf die korrekte Polarität achten.
- Entladene Batterien stets durch neue Batterien ersetzen.
- Batteriepacks dürfen nicht aufgeladen werden.

10.2.5 Entsorgung



Defekte oder verbrauchte Batteriepacks gemäß der Europäischen Richtlinie 2006/66/EG recyceln. Örtliche Bestimmungen zur getrennten Entsorgung von Batterien beachten.

Abbildungsverzeichnis

1.1	LSW mit allen Funktionen	1
1.2	LSW mit RFID Lesefeld (rot) und Transponderkarte (grün)	4
2.1	Notwendige Löcher für die Außeneinheit	7
2.2	Notwendige Löcher für die Inneneinheit	7
2.3	Montage der Außeneinheit	7
2.4	Montage der Inneneinheit	8
2.5	Montage der Inneneinheit	9
2.6	Montage der Inneneinheit	10
2.7	Rahmenposition (gestrichelt) für die korrekte Funktion des Abfrageschiebers. Riegel (rot), Abfrageschieber (grün), Türe (grau) und Schloss (blau)	11
8.1	Position der verschiedenen LEDs	35
8.2	Position der verschiedenen LEDs	37
8.3	Austausch der Batterie	44
8.4	Austausch der Nummernplatte	45
9.1	Technische Abmaße - Oben: Seitenansicht mit Türe (grau), Außeneinheit (rechts) und Inneneinheit (link) - Unten: Inneneinheit (links) und Außeneinheit (rechts)	47

Tabellenverzeichnis

1.1	Übersicht über die verschiedenen Bedienelemente	3
1.2	Übersicht über die verschiedenen kapazitiven Tasten	3
1.3	Übersicht über die verschiedenen Einbaurichtungen	5
2.1	Übersicht über die richtige Schraubenlänge abhängig von der Türstärke	8
8.1	Übersicht über die verschiedenen LED Statusmeldungen	35
8.3	Übersicht über die verschiedenen LED Statusmeldungen	37
8.5	Übersicht über die verschiedenen LED Statusmeldungen	39
8.7	Übersicht über die verschiedenen LED Statusmeldungen	41
9.1	Technische Daten	48