

Gantner Batterieschranksschlösser

Funktionsbeschreibung der batterieversorgten Schranksschlösser

GAT ECO.Side Lock



GAT ECO.Lock



GL7p



© Copyright 2026 Gantner Electronic GmbH

Alle Rechte vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigung einer Backup-Kopie von Software für den eigenen Gebrauch zu Sicherungszwecken, soweit dies technisch möglich ist und von uns empfohlen wird. Zuwiderhandlungen verpflichten zu Schadensersatz.

Haftung

Ansprüche gegenüber dem Hersteller in Anlehnung an die in diesem Handbuch beschriebenen Hard- und/oder Softwareprodukte richten sich ausschließlich nach den Bestimmungen der Garantie. Weitergehende Ansprüche sind ausgeschlossen, insbesondere übernimmt der Hersteller keine Gewähr über die Vollständigkeit und Richtigkeit des Inhaltes dieses Handbuches. Änderungen bleiben vorbehalten und können jederzeit auch ohne entsprechende Voranmeldung durchgeführt werden.

Warenzeichen

An dieser Stelle sei auf die in diesem Handbuch verwendeten Kennzeichnungen und eingetragenen Warenzeichen hingewiesen. Alle Produkt- oder Firmennamen, die in diesem Handbuch erwähnt werden, dienen lediglich Identifizierungs- und Erklärungszwecken und je nach Bezeichnung kann es sich dabei um Warenzeichen oder eingetragene Warenzeichen der entsprechenden Firmen handeln.

Kontakt

Bei Fragen in Zusammenhang mit diesem Produkt wenden Sie sich bitte an die für Sie zuständige Vertretung oder direkt an eine der Gantner Electronic GmbH Niederlassungen. Die Kontaktadressen sind mit folgendem Link aufrufbar: www.gantner.com/de/locations.

Kontaktadressen des Herstellers

Gantner Electronic GmbH
Bundesstraße 12
6714 Nüziders, Österreich

Wichtige Informationen

Verehrte Kundin, verehrter Kunde,

Damit unser Produkt in Ihrer Anlage zu Ihrer Zufriedenheit sicher und ohne Fehler arbeitet, weisen wir Sie auf folgende Grundregeln hin.

- > Beachten Sie die Sicherheitshinweise in diesem Handbuch. Diese werden durch die Signalwörter "GEFAHR", "WARNUNG", "ACHTUNG" gekennzeichnet und informieren Sie über mögliche gefährliche Situationen und wie Sie diese vermeiden können.
- > Beachten Sie auch Informationen, die mit dem Signalwort "HINWEIS" gekennzeichnet sind. Diese enthalten wichtige Informationen zur Vermeidung von Sachschaden.
- > Achten Sie auch auf die Symbole und Warnhinweise auf dem Produkt.
- > Lesen Sie alle Informationen in diesem Handbuch genau durch, bevor Sie das Gerät installieren und in Betrieb nehmen.
- > Sofern dies nicht an anderer Stelle speziell dokumentiert ist, liegt die Installation, Inbetriebnahme und Wartung des Produkts in der Verantwortung des Kunden.
- > Bewahren Sie dieses Handbuch an einem sicheren, für Nachschlagezwecke schnell zugänglichen Ort auf.

Schreibweise von Sicherheitsinformationen und Sicherheitssymbole

Dieses Handbuch enthält wichtige Sicherheitshinweise und Symbole zur Vermeidung von Personen- und Sachschäden. Diese Informationen und Symbole informieren den Anwender über gefährlichen Situationen und beschreiben den sicheren, sachgemäßen Umgang des Produkts. Die Sicherheitshinweise enthalten auch Informationen zur Vermeidung der gefährlichen Situationen. Lesen Sie diese Sicherheitshinweise unbedingt genau und handeln Sie danach. Die folgenden Zeilen beschreiben die Struktur der in diesem Handbuch verwendeten Sicherheitshinweise und die Bedeutung der verwendeten Symbole.

1 Sicherheitshinweise zu Personenschaden

Sicherheitshinweise enthalten ein Signalwort, und beschreiben die Art der Gefahr und wie Sie diese Gefahr vermeiden können.



Wird das Sicherheitsalarmzeichen ohne Signalwort verwendet, folgen immer wichtige sicherheitsrelevante Informationen, die genau gelesen und befolgt werden müssen. Nichtbeachtung kann zu Personenschaden führen.

Format von Sicherheitshinweisen, die sich auf einen ganzen Abschnitt beziehen:

Die Verwendung dieses Sicherheitshinweises ist mit oder ohne Symbol möglich.

VORSICHT



Elektrischer Schlag.

- Das Berühren von spannungsführenden Teilen kann zu Verletzungen durch elektrischen Schlag führen.
- Schutzeinrichtungen und Abdeckungen nicht entfernen.
 - Anschlussklemmen nicht berühren, wenn das Produkt mit Strom versorgt wird.

Format von Sicherheitshinweisen, die im Text eingebettet sind und sich auf diese konkrete Stelle beziehen:

ACHTUNG! Elektrischer Schlag. Schutzeinrichtungen und Abdeckungen nicht entfernen. Anschlussklemmen nicht berühren, wenn das Produkt mit Strom versorgt wird.

2 Sicherheitshinweise zu Sachschaden

Sicherheitshinweise, die mögliche Gefahrensituationen für Sachschaden beschreiben, haben dasselbe Layout wie Sicherheitshinweise für Personenschaden, nur dass als Signalwort "HINWEIS" verwendet wird.

Format von Sicherheitshinweisen, die sich auf einen ganzen Abschnitt beziehen:

HINWEIS

Gefahr von Sachschaden für das Gerät und angeschlossener Geräte.



Gefahr von Fehlfunktion.

- Folgende Anweisungen genau lesen und befolgen, bevor Sie das Gerät installieren.
- Immer die Anweisungen befolgen.






Format von Sicherheitshinweisen, die im Text eingebettet sind und sich auf diese konkrete Stelle beziehen:








HINWEIS! Gefahr von Sachschaden für das Gerät und angeschlossener Geräte. Lesen Sie die folgenden Anweisungen genau, bevor Sie das Gerät installieren.

3 Bedeutungen verwendeter Signalwörter

	Kennzeichnet eine gefährliche Situation die, wenn sie nicht vermieden wird, zu leichten und mittelschweren Verletzungen führen kann.
	Kennzeichnet wichtige Informationen, die jedoch nicht verletzungsrelevant sind (z. B. Hinweise bezüglich möglichen Sachschaden).

4 Bedeutungen verwendeter Sicherheitsymbole

	Vorsicht: Allgemeine Information Dieses Symbol kennzeichnet allgemeine Warnungen, die sich nicht auf einen bestimmten Typ von Gefahren beziehen.
	Vorsicht: Elektrischer Schlag Dieses Symbol kennzeichnet Warnungen in Bezug auf elektrische Gefahren (gefährliche Spannungen und Ströme).
	Verbot: Nicht auseinander nehmen, nicht demontieren Dieses Symbol kennzeichnet Warnungen bezüglich nicht erlaubten auseinander nehmen und Demontage von bestimmten Teilen oder Geräten. Nichtbefolgung kann zu Beschädigungen oder Fehlfunktionen des Geräts führen.
	Verpflichtende Tätigkeit: Allgemeine Information Dieses Symbol kennzeichnet allgemeine Informationen die gelesen und befolgt werden müssen, bevor weitere Schritte durchgeführt werden.
	Verpflichtende Tätigkeit: Instruktionen lesen Dieses Symbol kennzeichnet Informationen, die sich auf wichtige Instruktionen beziehen, die in diesem Handbuch oder an einem anderen Ort zu finden sind. Diese Texte müssen gelesen und befolgt werden.

 Wichtige Sicherheitshinweise 	
 	<ul style="list-style-type: none"> - Die Installation, Inbetriebnahme und Wartung unserer Geräte hat durch entsprechendes Fachpersonal zu erfolgen. Insbesondere elektrische Anschlüsse dürfen nur vom fachkundigen Personal ausgeführt werden. Dabei sind die Installationsvorschriften nach den einschlägigen, nationalen Errichtungsbestimmungen (z.B. ÖVE, VDE, ...) zu beachten. <ul style="list-style-type: none"> ➔ Arbeiten durch unqualifiziertes Personal kann zu Verletzungen führen (z. B. elektrischer Schlag). - Wenn nicht anders angegeben, hat die Installation und Wartung unserer Geräte ausschließlich im spannungsfreien Zustand zu erfolgen. Dies gilt insbesondere bei Geräten, die an das Niederspannungsnetz angeschlossen sind. <ul style="list-style-type: none"> ➔ Wenn das Gerät nicht von der Versorgungsspannung getrennt ist, kann es durch Berührung von Klemmen oder internen Teilen zu leichten Verletzungen kommen (elektrischer Schlag).
	<ul style="list-style-type: none"> - Es ist untersagt, Veränderungen am Produkt vorzunehmen (Gerät, Anschlusskabel): <ul style="list-style-type: none"> ➔ Veränderungen am Produkt können zu Verletzungen oder Sachschaden führen und das Gerät beschädigen. - Es ist untersagt, Schutz- und Abdeckhauben von Geräten zu entfernen. <ul style="list-style-type: none"> ➔ Das Entfernen von Schutz- und Abdeckhauben vom Produkt können zu Verletzungen oder Sachschaden führen. - Versuchen Sie nicht, Produkte nach einem Defekt, einem Fehler oder einer Beschädigung eigenmächtig zu reparieren oder wieder in Betrieb zu nehmen. Kontaktieren Sie in diesem Fall unbedingt Ihren Kundenberater oder die Hotline der Gantner Electronic GmbH.
 	<ul style="list-style-type: none"> - Installation, Inbetriebnahme, Betrieb und Wartung des erworbenen Produkts haben bestimmungsgemäß, d.h. innerhalb der in der zugehörigen Produktdokumentation aufgeführten technischen Einsatzbedingungen, zu erfolgen. Lesen Sie daher unbedingt die entsprechenden Kapitel in diesem Handbuch durch und handeln Sie danach. - Falls dennoch einzelne Punkte unklar sein sollten, handeln Sie nicht „auf gut Glück“, sondern fragen Sie bei dem für Sie zuständigen Kundenberater oder bei der Hotline der Gantner Electronic GmbH nach. - Kontrollieren Sie direkt nach Erhalt der Ware die Verpackung und das Produkt bzw. den Datenträger optisch auf seine Unversehrtheit. Kontrollieren Sie die Lieferung auch auf ihre Vollständigkeit (-> Zubehörteile, Dokumentation, Hilfsmittel etc.). - Würde die Verpackung durch den Transport beschädigt oder sollten Sie einen Verdacht auf eine Beschädigung oder Fehlfunktion des Produkts haben, darf das Produkt nicht in Betrieb genommen werden. Kontaktieren Sie in diesem Fall Ihren Kundenberater. Er wird bemüht sein, so schnell wie möglich Abhilfe zu schaffen. - Wenn nicht anders festgelegt, trägt der Kunde die Verantwortung für bestimmungsgemäße Installation, Inbetriebnahme, Betrieb und Wartung des Produkts. - Die Gantner Electronic GmbH übernimmt keine Verantwortung für Verletzungen oder Schäden, die Folge eines unsachgemäßen Gebrauches sind.

Auch wenn wir uns um Sorgfalt und stetige Verbesserung bemühen, können wir nicht ausschließen, dass sich Fehler in unsere Dokumentationen einschleichen. Wir weisen daher darauf hin, dass die Gantner Electronic GmbH keine Gewähr für die Vollständigkeit und Richtigkeit des Inhaltes dieses Handbuchs übernimmt. Änderungen bleiben vorbehalten und können jederzeit, auch ohne entsprechende Voranmeldung, von uns durchgeführt werden.

Wenn Sie auf Fehler am Produkt oder in der produktbegleitenden Dokumentation stoßen oder wenn Sie Verbesserungsvorschläge haben, wenden Sie sich bitte vertrauensvoll an Ihren Kundenberater oder direkt an die Gantner Electronic GmbH.

Aber auch wenn Sie uns nur mitteilen wollen, dass alles reibungslos funktioniert hat, sind wir über Ihre Nachricht erfreut.



Eine Übersicht aller Zulassungen der Batterieschlösser finden Sie im Partner-Bereich auf der Gantner Website: <https://www.gantner.com>

INHALTSVERZEICHNIS

1	EINLEITUNG	9
1.1	Zu diesem Handbuch	9
1.2	Kapitelübersicht.....	9
1.3	Zielgruppen.....	9
1.4	Formatierungen.....	10
1.4.1	Sicherheitskritische Informationen	10
1.4.2	Nicht sicherheitskritische Informationen.....	10
1.4.3	Anweisungen und Resultate	10
1.5	Ansprechpartner bei Rückfragen	10
1.6	Begriffsdefinition.....	11
2	KONFIGURATION	13
2.1	Allgemeine Informationen	13
2.2	Konfiguration mit GAT ECO Lock Configurator	14
2.2.1	Konfiguration aus einem Schloss lesen.....	15
2.2.2	Konfigurationseinstellungen bearbeiten und in ein Schloss schreiben.....	16
2.2.3	Firmware in ein Schloss laden.....	17
2.3	Konfiguration mit der MoLA App	18
2.4	Konfigurationseinstellungen.....	19
2.4.1	Betriebsmodus	19
2.4.2	Schranknummer	19
2.4.3	Akustische Signale.....	19
2.4.4	Automatische Öffnungsfunktion	20
2.4.5	Nutzungsdauer.....	20
2.4.6	Persönliche Schränke ohne Datenträger sperren	21
2.4.7	RF-Standards	21
2.4.8	MASTER Datenträger	21
2.4.9	Funkschnittstelle	22
2.4.10	Alarmmodus (GAT ECO.Side Lock).....	22
2.4.11	PIN-Code Tastatur (GL7p).....	22
2.4.12	Konfigurationseinstellungen	23
3	BEDIENUNG	27
3.1	Zielgruppe.....	27
3.2	Allgemein.....	27
3.3	PIN-Code Bedienung (GL7p).....	28
3.4	Alarmbehandlung (GAT ECO.Side Lock).....	28
3.5	Automatischer Antennenabgleich (GAT ECO.Side Lock).....	29
3.5.1	Antennenabgleich mit dem SERVICE Datenträger	29
3.5.2	Antennenabgleich über GAT ECO Lock Configurator	29
3.6	Betriebsmodi.....	30
3.6.1	Free Locker Modus (mit oder ohne die Nutzungsdauerfunktion).....	31
3.6.2	Free Locker Universal Modus	32
3.6.3	Free Locker Unique Number Modus.....	33
3.6.4	Personal Locker Programming Card Modus	34
3.6.5	Personal Locker Expiry Date Modus	37
3.7	GAT ECO.Basic Set.....	38
3.8	Informationen zu den Systemdatenträgern.....	39
3.8.1	MASTER Datenträger	39
3.8.2	OPEN MASTER Datenträger (Optionales Zubehör).....	40
3.8.3	DELETE MASTER Datenträger	40
3.8.4	PROGRAM Datenträger.....	40

3.8.5	BATTERY Datenträger.....	40
3.8.6	SERVICE Datenträger.....	40
3.8.7	APP KEY Datenträger.....	41
3.8.8	BLOCKING Datenträger (optionales Zubehör).....	41
3.9	Übersicht der Signalisierung.....	42

1 EINLEITUNG

1.1 Zu diesem Handbuch

Dieses Handbuch enthält die notwendigen Informationen für die Konfiguration und den Betrieb der batterieversorgten, elektronischen Schranksschlösser von Gantner. Die folgenden Gantner Batterieschrankschlösser (in dieser Anleitung auch kurz Batterieschlösser genannt) werden in dieser Anleitung behandelt:

GAT ECO.Side Lock

Alle Varianten außer GAT ECO.Side Lock 7000 NW BA CardNET und GAT ECO.Side Lock 7000 NW BA OSS.

GAT ECO.Lock

Alle Varianten außer GAT ECO.Lock 7100 NW BA CardNET und GAT ECO.Lock 7100 NW BA OSS.

GL7p

Alle Varianten außer GL7p.x30x CardNET und GL7p.x30x OSS.

In diesem Handbuch werden die Begriffe "Batterieschloss" und "Schloss" für alle Schlossvarianten verwendet. Wenn sich Informationen in der Anleitung nur auf ein bestimmtes Schloss beziehen, wird der jeweilige Produktname verwendet.



Informationen zur Installation und Inbetriebnahme der Batterieschlösser finden Sie in einem separaten Installationshandbuch (das Handbuch "INSTALL" der jeweiligen Schlossvariante).



Informationen über die Konfiguration und den Betrieb der Batterieschlösser mit CardNET- und OSS-Funktionalität finden Sie in den separaten CardNET- und OSS-Handbüchern.

1.2 Kapitelübersicht

Im Kapitel 2 "KONFIGURATION" finden Sie Informationen darüber, wie das Schloss mit der Konfigurationssoftware GAT ECO Lock Configurator und mit der MoLA App konfiguriert wird. Hier werden die wichtigsten Konfigurationseinstellungen des Schlosses erklärt und eine Tabelle mit allen Einstellungen ist ebenfalls verfügbar.

Im Kapitel 3 "BEDIENUNG" werden die verschiedenen Betriebsmodi des Schlosses beschrieben. Auch die zur Wartung der Schließanlage benötigten Systemdatenträger und die LED-Signalisierung werden in diesem Kapitel erläutert.

1.3 Zielgruppen

Dieses Handbuch enthält die notwendigen Informationen für die verschiedenen Lebenszyklen der Batterieschlösser. Wenn nicht ausdrücklich angegeben, sind die Informationen generell für alle Zielgruppen bestimmt. Wenn ein Kapitel für eine bestimmte Zielgruppe bestimmt ist, wird diese zu Beginn des Kapitels angegeben.

Die folgenden Zielgruppen finden Informationen in diesem Handbuch:

- > Installationstechniker (Konfiguration)
- > Betreiber von Schrankanlagen (Betrieb)



ACHTUNG! Verletzung und Sach-/Geräteschaden. Die Tätigkeiten, die laut diesem Handbuch für eine bestimmte Zielgruppe bestimmt sind, dürfen nur von dieser Zielgruppe ausgeführt werden. Ausführen der Tätigkeiten durch unqualifiziertes Personal kann zu Verletzungen oder Sach-/Geräteschaden führen.

1.4 Formatierungen

1.4.1 Sicherheitskritische Informationen

Zur Anzeige von wichtigen, sicherheitskritischen Informationen wird in diesem Handbuch folgende Formatierung verwendet (mit Beispieltext):

HINWEIS! Nach diesem Signalwort folgt in diesem Handbuch ein Hinweistext, den Sie unbedingt lesen und befolgen müssen. Der Hinweistext enthält wichtige Informationen. Nichtbeachtung kann zu Sachschaden führen.

Diese Hinweise sind unbedingt zu lesen und zu befolgen.

1.4.2 Nicht sicherheitskritische Informationen

Zur Anzeige von wichtigen, aber nicht sicherheitskritischen Informationen wird in diesem Handbuch folgende Formatierung verwendet (mit Beispieltext):



Der Text neben diesem Symbol enthält interessante Informationen über den aktuellen Abschnitt. Sie müssen diesen Text nicht unbedingt lesen, die Informationen helfen Ihnen aber, die Beschreibung in diesem Abschnitt besser zu verstehen oder geben interessante Tipps für das beschriebene Gerät oder die Bedienung der Software.

1.4.3 Anweisungen und Resultate

Aktionsschritte, die der Benutzer ausführen muss, und die Resultate dieser Aktionen werden wie folgt formatiert.

- ▶ Nach diesem Symbol steht eine Handlungsaufforderung, die Sie ausführen sollen.
 - Dieses Symbol kennzeichnet das Resultat nach Ausführung des vorigen Handlungsschrittes.

1.5 Ansprechpartner bei Rückfragen

Bei Fragen in Zusammenhang mit den Gantner Batterieschrankschlössern wenden Sie sich bitte an die für Sie zuständige Vertretung oder direkt an eine der Gantner Electronic GmbH Niederlassungen. Die Kontaktadressen sind mit folgendem Link aufrufbar: www.gantner.com/de/locations.

1.6 Begriffsdefinition

Einige Begriffe werden in diesem Handbuch öfters verwendet und sind wie folgt definiert.

Computer / PC

Diese Begriffe bezeichnen alle Desktop- und Laptop-Computer, die zur Konfiguration und Wartung der Schlösser verwendet werden.

Datenträger

Ein Ausweismedium mit elektronischem Speicher und einer ID-Nummer, das von den Mitarbeitern und Besuchern einer Anleitung zur Identifizierung verwendet wird. Datenträger gibt es in verschiedenen Formen (z. B. Chipkarten, Armbänder, Schlüsselanhänger) und für unterschiedliche RFID-Technologien (LEGIC, MIFARE®, ISO 15693, HID iCLASS).

Systemdatenträger

Verschiedene Systemdatenträger werden für die Programmierung und für Service- und Wartungsaufgaben an den Schrankschlössern eingesetzt. Diese Datenträger haben spezielle Funktionen. Da die Systemdatenträger für die Bedienung der Schrankschlösser unbedingt benötigt sind und sicherheitskritische Funktionen haben, müssen diese an einem sicheren, vor unbefugtem Zugriff geschützten Ort aufbewahrt werden. Die meisten Systemdatenträger sind im GAT ECO.Basic Set enthalten. Einige müssen, falls benötigt, separat bestellt werden.

FID (Firmen-ID) und Site Key

LEGIC Systeme verwenden die FID Nummer, in MIFARE® Systemen wird der Site Key verwendet, welcher eine Kombination von FID und den Lese- und Schreibschlüsseln ist. Die FIDs und die Site Keys sind Unikate für jede Anlage. Diese Nummern sind in allen Datenträgern und allen Geräten codiert und dadurch wird sichergestellt, dass ein Datenträger nicht in verschiedenen Anlagen verwendet wird.

GAT ECO Lock Configurator

Eine Gantner PC-Software, die zur Konfiguration der Batterieschlösser von Gantner verwendet wird.

Schloss / Schrankschloss / Batterieschloss

Allgemeine Bezeichnung für alle Varianten der elektronischen Gantner Schlösser.

Schrank

Der Begriff "Schrank" bezeichnet hier allgemein einen Umkleideschrank, ein Depot, ein Schließfach oder Ähnliches, das mit einem Gantner Batterieschrankschloss versperrt wird.

RFID (Radio-Frequency Identification = Identifizierung mit Hilfe elektromagnetischer Felder)

Bezeichnet in diesem Handbuch die Identifizierung einer Person über Funk im Nahbereich. Als Ausweismedium dient dazu ein RFID Datenträger, z. B. in Form eines Armbands oder einer Chipkarte.

Funk (BLE)

Identifikation über eine Funkschnittstelle im Bereich 2,402 bis 2,48 GHz, über die eine Identifikation und Schrankbedienung aus mehreren Metern, z. B. mittels einer App auf einem Smartphone, möglich ist. Funk bedeutet in diesem Handbuch auch BLE. Ein zusätzliches Feature ist die Überwachung des Schlossstatus über einen Access Point und die Locker Management Software eLoxx Relaxx.

Benutzer / Gast / Besucher

Diese Begriffe bezeichnen in diesem Handbuch die Anwender (Personen) in einer Anlage, die einen Schrank mit Gantner Batterieschrankschloss bedienen (öffnen oder versperrern), die Datenträger nutzen oder andere Gantner Produkte bedienen.

2 KONFIGURATION

2.1 Allgemeine Informationen

Die batteriebetriebenen Schrankschlösser von Gantner werden mit einem PC/Laptop und der GAT ECO Lock Configurator Software oder mit der MoLA App auf einem mobilen Gerät konfiguriert. Bei Schlössern, die dieselben Konfigurationseinstellungen verwenden, wird zunächst eine Konfigurationsdatei erstellt und in GAT ECO Lock Configurator gespeichert. Die Konfigurationsdatei kann dann auf jedes Schloss übertragen werden, das dieselbe Konfiguration benötigt. Für Schlösser, die eine andere Konfiguration benötigen, muss eine separate Konfiguration in GAT ECO Lock Configurator erstellt werden.



Prüfen Sie bei der Konfiguration des Schlosses immer, ob die neueste Firmware installiert ist. Falls nicht, aktualisieren Sie bitte vor der ersten Konfiguration die Firmware auf die aktuelle Version. Siehe Kapitel "2.2.3. Firmware in ein Schloss laden".

Eine weitere Möglichkeit ist die Konfiguration mittels der MoLA App auf einem Mobilgerät. Die MoLA App kann vom Google Playstore heruntergeladen werden und ist auf Mobilgeräten mit Android Betriebssystem lauffähig. Für die Konfiguration verwendet die App NFC, d.h. das Mobilgerät muss NFC Kommunikation unterstützen. Mehr Details erfahren Sie unter "2.3. Konfiguration mit der MoLA App".

HINWEIS! Führen Sie nach der Konfiguration des ersten Schlosses einen kompletten Funktionstest durch, ob die Datenträger (MASTER Datenträger und Standarddatenträger für die Benutzer) am Schloss sicher gelesen werden und das Schloss die konfigurierte Funktionalität ausführt bevor sie diese Konfiguration dann bei den restlichen Schlössern anwenden.

Bei der Konfiguration werden unter anderem folgende Daten in das Schloss übernommen:

- > Kundenspezifische Anlagennummer
- > Schranknummer
- > Modus des Schlosses
- > Datenträgereinstellungen
- > Datum und Uhrzeit
- > MASTER Datenträger (und OPEN MASTER Datenträger, falls verwendet)



Die MASTER und OPEN MASTER Datenträger können auch direkt an einem Schloss einprogrammiert werden (siehe Abschnitt "3.8.1. MASTER Datenträger"). Aus Effizienzgründen wird jedoch empfohlen, die Datenträger mittels PC und GAT ECO Lock Configurator oder mit der MoLA App einzuprogrammieren.

HINWEIS! Die Schlösser stellen keine automatische Sommerzeitschaltung ein! Dies ist bei der Auswertung der Buchungen wie auch beim Berechtigen von Datenträgern mit Gültigkeitsdatum zu beachten!

2.2 Konfiguration mit GAT ECO Lock Configurator

Die GAT ECO Lock Configurator Software kann die Konfiguration eines Schlosses lesen. Die Einstellungen können dann bei Bedarf geändert und auf das Schloss hochgeladen werden. Es ist auch möglich, die Buchungsdaten auszulesen und die Firmware des Schlosses zu aktualisieren.

Um die Konfiguration zu starten, muss das Schloss mit dem entsprechenden USB-Kabel (z.B. das Kabel im GAT ECO.Basic Set) an den Computer angeschlossen und der Konfigurationsmodus über den SERVICE-Datenträger aktiviert werden (siehe "3.8.6. SERVICE Datenträger").

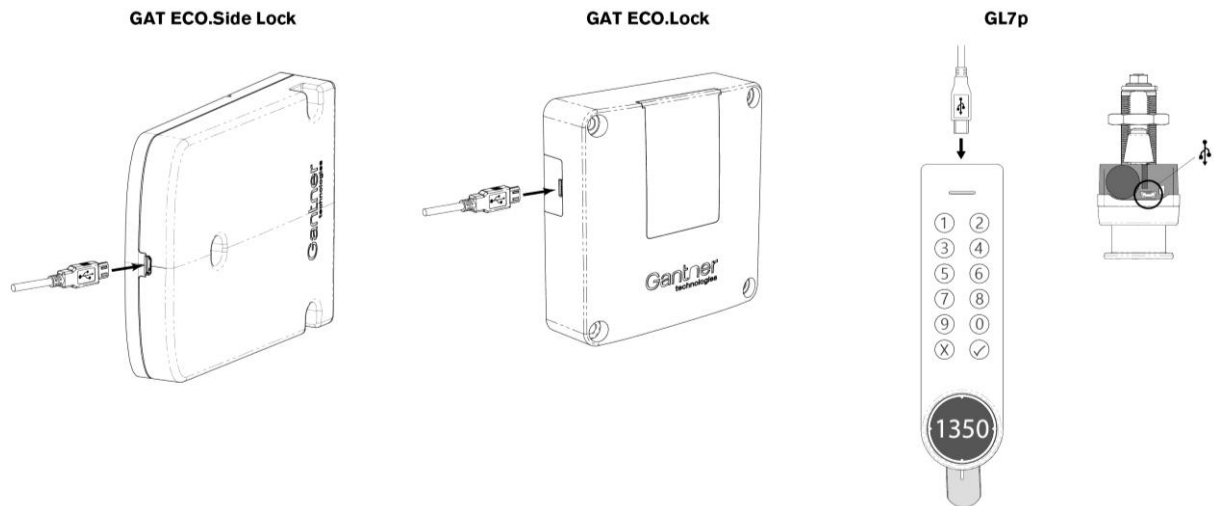


Bild 2.1 – USB-Anschluss der Schrankschlösser

HINWEIS! Die GL7p Schlösser werden durch das USB-Kabel mit Strom versorgt, weshalb die Batterie während der Konfiguration nicht im Schloss eingelegt sein muss. Achten Sie aber darauf, dass das Schloss nicht länger als 1 Minute stromlos ist (z. B. nach Abstecken des USB-Kabels bis zum Einlegen der Batterie), da ansonsten die Uhrzeit und das Datum gelöscht werden.



Es gibt eine separate Anleitung mit detaillierten Informationen zu den einzelnen Funktionen in GAT ECO Lock Configurator. Die GAT ECO Lock Configurator Software ist aktuell nur in englischer Sprache verfügbar.

2.2.1 Konfiguration aus einem Schloss lesen

- ▶ Starten Sie GAT ECO Lock Configurator. Die Verknüpfung ist bei Standard-Installation im Windows Menü unter der Gruppe "Gantner Electronic GmbH" zu finden.
 - Der Start der Software dauert einige Sekunden. Danach wird das Hauptfenster angezeigt.

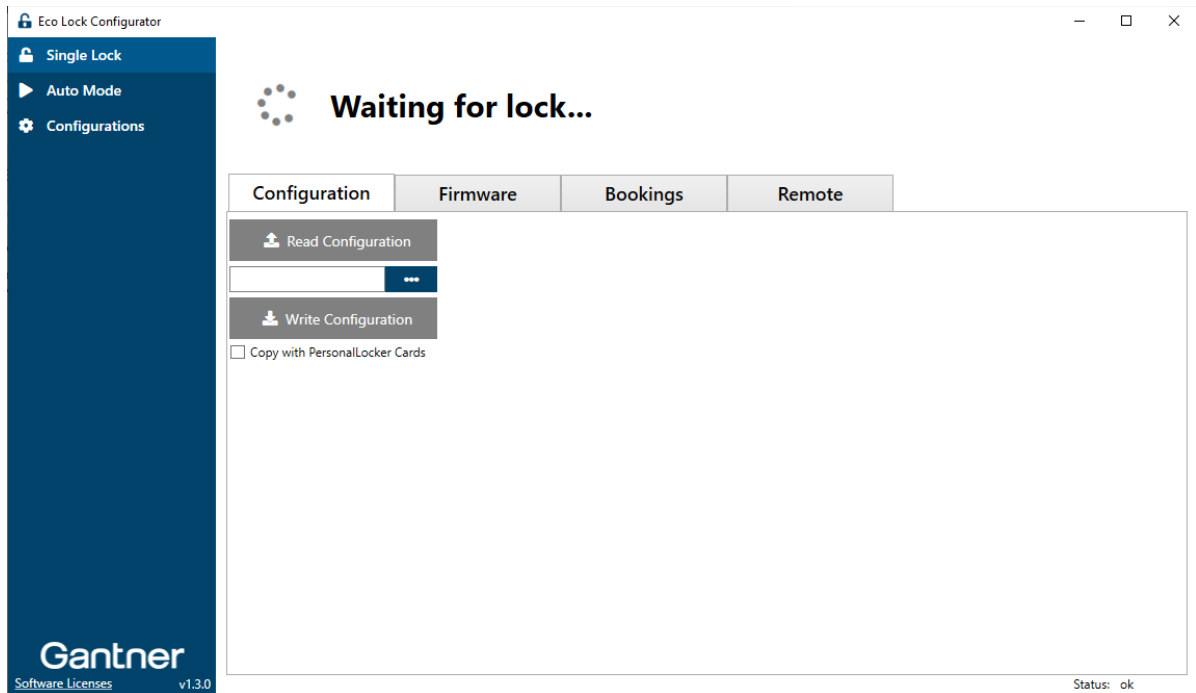


Bild 2.2 – Hauptbildschirm von GAT ECO Lock Configurator



Die Software ist nur in Englisch verfügbar.

- ▶ Wählen Sie links den Menüpunkt "Single Lock" aus.
- ▶ Wechseln sie zur Registerkarte "Configuration".
- ▶ Schließen Sie das Schloss über USB an den PC an (siehe Bild 2.1).
- ▶ Wenn das Schloss schon für eine Kundenanlage mit dem spezifischen Site Key konfiguriert ist, blinkt die LED am Schloss rot/grün. Lesen Sie den SERVICE Datenträger am Schloss, um die Kommunikation zu aktivieren (siehe "3.8.6. SERVICE Datenträger").
Falls das Schloss noch nicht mit einem kundenspezifischen Site Key konfiguriert wurde, blinkt die LED am Schloss grün und die Kommunikation ist ohne SERVICE Datenträger möglich.
 - Die Konfigurationseinstellungen werden aus dem Schloss gelesen und angezeigt.

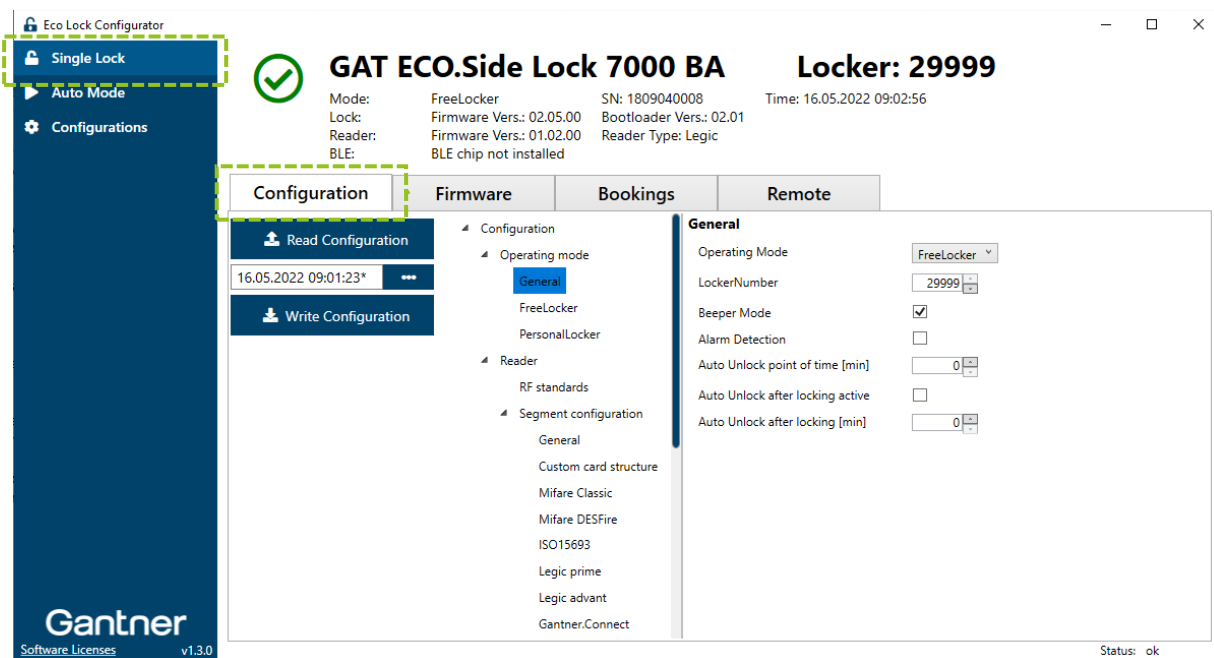
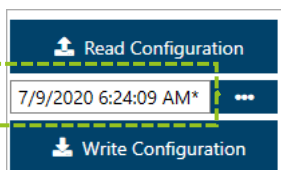


Bild 2.3 – Konfigurationseinstellungen

Im linken Bereich des Konfigurationsfensters sehen Sie die Konfigurationskategorien als Baumstruktur. Bei Auswahl einer Kategorie (im Beispiel "General") werden rechts die Konfigurationseinstellungen der Kategorie angezeigt.



Den Namen der aktuell angezeigten Konfiguration sehen Sie im Textfeld links des Konfigurationsbaums. Nach dem Lesen einer Konfiguration aus einem Schloss steht hier das aktuelle Datum und die Uhrzeit. Beim Speichern der Konfiguration (siehe folgende Schritte) können Sie diesen Namen ändern.

Wenn Sie eine zuvor gespeicherte Konfiguration geladen haben, wird hier der Name der gespeicherten Konfiguration angezeigt.

2.2.2 Konfigurationseinstellungen bearbeiten und in ein Schloss schreiben



Eine Beschreibung der einzelnen Konfigurationseinstellungen finden Sie im Kapitel "2.4.12. Konfigurationseinstellungen".

- ▶ Bearbeiten Sie die gewünschten Einstellungen.
 - Die Änderungen werden automatisch gespeichert.
- ▶ Zum Übertragen der Einstellungen in das Schloss klicken Sie auf die Schaltfläche "Write Configuration".
 - Die Änderungen werden in das Schloss geladen. Am Schloss blinkt die LED kurz rot auf.
 - Während der Übertragung wird die Windows Ladeanzeige (Standard: Ladekreis als Mauszeiger) angezeigt.
- ▶ Mit Klick auf "Read Configuration" kann die Konfiguration erneut aus dem Schloss gelesen werden.
- ▶ Zum Speichern der aktuell angezeigten Konfiguration klicken Sie auf die Schaltfläche und wählen Sie im Pop-Up Menü "Save/Load Configuration".
 - Die Seite mit den bereits gespeicherten Konfigurationen wird angezeigt. Hier können Sie die Konfiguration speichern und in die Konfigurationsbibliothek einsortieren.

2.2.3 Firmware in ein Schloss laden

Die Firmware ist das "Betriebssystem" eines Schlosses und durch das Laden von neuen Firmware-Versionen können neue Funktionsmöglichkeiten für das Schloss hinzugefügt oder auch eventuell auftretende Probleme behoben werden.

HINWEIS! Prüfen Sie immer, ob die neueste Firmware im Schloss installiert ist, und aktualisieren Sie diese bei Bedarf. Die neueste Firmware wird nur mit einer aktiven FTP-Verbindung zum Internet aktualisiert, wenn der GAT ECO Lock Configurator gestartet wird.

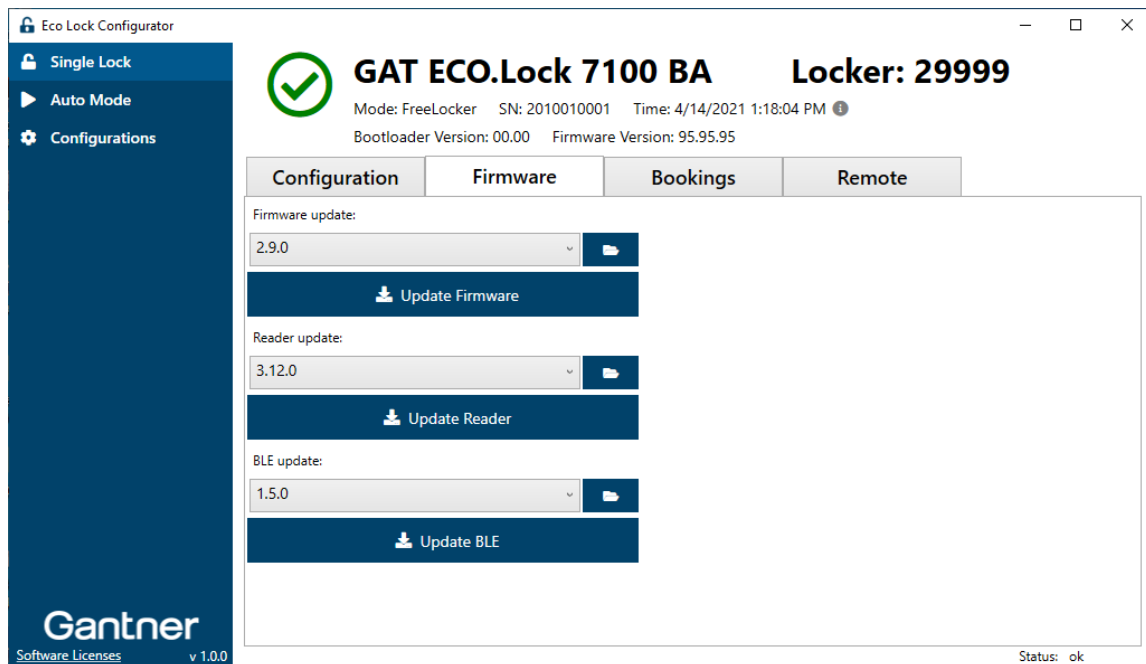



Bild 2.4 – Konfigurationseinstellungen

- ▶ Stellen Sie sicher, dass das Schloss über USB mit dem PC verbunden ist.
- ▶ Wechseln Sie im Menü "Single Lock" auf die Registerkarte "Firmware".
 - Die möglichen Firmware-Typen werden erkannt und Sie können die gewünschten Versionen auswählen.
- ▶ Wenn Sie nur die Version auswählen, wird die passende Firmware von GAT ECO Lock Configurator verwendet.
- ▶ Wenn Sie eine spezielle Firmware verwenden möchten, klicken Sie auf das Symbol  und wählen Sie die gewünschte Firmware-Dateien aus.
- ▶ Klicken Sie auf "Update Firmware", "Update Reader" oder "Update BLE", um die gewünschte Komponente mit der gewählten Firmware zu beladen.
 - Eine Grafik zeigt den Fortschritt des Beladens an, was einige Sekunden dauern kann.
 - Während dem Beladen mit einer Firmware blinkt am Schloss die rote LED.
 - Nach erfolgreichem Update erhalten Sie eine entsprechende Erfolgsmeldung.

2.3 Konfiguration mit der MoLA App

MoLA App, die vom Google Play Store geladen werden kann, haben Sie die Möglichkeit, das Schloss mittels eines Mobilgeräts (z. B. Smartphone) zu konfigurieren. Für die Verwendung der MoLA App sind folgende Voraussetzungen zu erfüllen:

- > Mobilgerät mit Android Betriebssystem Version 4.4.0 oder neuer
- > Das Mobilgerät muss NFC unterstützen
- > Das Mobilgerät darf nicht gerootet sein
- > Im Schloss muss die neueste Firmware-Version installiert sein
- > Ein gültiger APP KEY Datenträger ist für die Konfiguration von Schlössern vor Ort notwendig

Die MoLA App kann vom Google Play Store mit folgendem Link geladen werden:



<https://play.google.com/store/apps/details?id=com.gantner.mola>



Aufgrund technischer Einschränkungen in iOS kann die MoLA App zur Zeit nicht auf Geräten von Apple verwendet werden.

In MoLA können Sie dieselben Konfigurationseinstellungen wie in GAT ECO Lock Configurator vornehmen (siehe "2.4. Konfigurationseinstellungen"). Eine genaue Bedienungsanleitung der App finden Sie in der MoLA App selbst.

Der APP KEY Datenträger ist ein spezieller Systemdatenträger (siehe "3.8. Informationen zu den Systemdatenträgern") und ist im GAT ECO.Basic Set enthalten. Dieser Datenträger ist notwendig, um die Konfiguration eines Schlosses zu ändern oder eine neue Konfiguration zu erstellen.



Wenn ein Schloss auf Werkseinstellung gesetzt ist (Auslieferungszustand mit noch keiner gespeicherten Konfiguration) ist das Schloss im "DEMO" Modus und der APP KEY Datenträger nicht notwendig.

Ist der APP KEY Datenträger in MoLA geladen, bleibt dieser eine bestimmte Zeit lang gültig. Wenn die Gültigkeit abgelaufen ist, wird der APP KEY Datenträger automatisch vom Schloss gelöscht. Dies beugt einem unerlaubten Zugriff von Fremd-Apps, Malware, etc. auf den APP KEY Datenträger vor.

2.4 Konfigurationseinstellungen

Die wichtigsten Konfigurationseinstellungen, die in GAT ECO Lock Configurator eingestellt werden können, sind im folgenden Abschnitt erläutert. Eine Liste und kurze Erläuterung der einzelnen Konfigurationseinstellung des Schlosses finden Sie im Abschnitt "2.4.12. Konfigurationseinstellungen".



Die verfügbaren Konfigurationseinstellungen hängen davon ab, welche Schlossvariante konfiguriert wird. Die PIN-Code-Einstellungen sind zum Beispiel nur für das GL7p relevant.

2.4.1 Betriebsmodus

Das Schloss kann in einem von fünf verschiedenen Betriebsmodi betrieben werden. Siehe "3.6. Betriebsmodi" für eine detaillierte Beschreibung der einzelnen Modi. Diese Einstellung finden Sie hier:

Configuration > Operating mode > General > Operating Mode

- ▶ Aus dem Menü "Operating Mode", wählen Sie
 - > "Free locker"
 - > "Free locker universal"
 - > "Personal locker programming card"
 - > "Personal locker expiry date"
 - > "Free locker unique number"

2.4.2 Schranknummer

Die Schranknummer des Schanks, in dem das Schloss installiert ist, kann definiert werden. Diese Einstellung finden Sie hier:

Configuration > Operating mode > General > LockerNumber

- ▶ Geben Sie die Schranknummer für das Schloss im Feld "Locker number" ein.

2.4.3 Akustische Signale

Das Schloss hat einen integrierten Piepser, der bei einer Bedienung oder für bestimmte Meldungen einen Ton erzeugt. Sie können diese Töne aktivieren oder deaktivieren. Diese Einstellung finden Sie hier:

Configuration > Operating mode > General > Beeper Mode

- ▶ Aktivieren / deaktivieren Sie die "Beeper Mode" Option, um die Funktion ein-/auszuschalten.
HINWEIS! Wenn deaktiviert, werden die akustische Signale trotzdem weiterhin erzeugt, wenn ein Alarm ausgelöst wird und wenn ein Systemdatenträger am Schloss verwendet wird, z. B., um die Tür mit einem MASTER Datenträger zu öffnen.

2.4.4 Automatische Öffnungsfunktion

Für die Schlösser stehen zwei automatische Öffnungsfunktionen zur Verfügung. Die erste Funktion entriegelt den Schrank automatisch zu einem definierten Zeitpunkt am Tag. Die zweite Funktion entriegelt den Schrank automatisch eine definierbare Anzahl von Minuten nach dem Verriegeln. Für beide Funktionen muss die Zeit einmalig per Software korrekt eingestellt werden.

HINWEIS! Wenn eine dieser beiden Funktionen aktiviert ist, wird das Schloss unabhängig vom Betriebsmodus immer zum definierten Zeitpunkt entriegelt.

HINWEIS! Die Schlösser arbeiten immer nach der UTC-Zeit und passen sich nicht automatisch z. B. an Sommer-/Winterzeit an. Wählen Sie daher eine Zeit, die für die Öffnung des Schlosses zu jeder Jahreszeit geeignet ist!

Die "automatische Öffnungsfunktion zu einem bestimmten Zeitpunkt" finden Sie hier:

Configuration > Operating mode > General > Auto Unlock point of time [min]

- ▶ Geben Sie hier den gewünschten Zeitpunkt in Minuten ab Mitternacht ein. Der Countdown zur Entriegelung beginnt also um 00:00 Uhr (24 h). Beispielweise bedeutet ein Wert von "300", dass das Schloss um 05.00 Uhr entriegelt wird. Ein Wert von "0" bedeutet, dass die Funktion inaktiv ist.

Die "automatische Öffnungsfunktion nach Verriegelung" finden Sie hier:

Configuration > Operating mode > General > Auto Unlock after locking active [min]

- ▶ Aktivieren / deaktivieren Sie die Option "Auto Unlock after locking active", um die Funktion ein-/auszuschalten.
- ▶ Geben Sie im Feld "Auto Unlock after locking active [min]" die Anzahl der Minuten für die Countdown-Zeit ein. Die Countdown-Zeit für die Entsperrung beginnt nach dem Verriegeln des Schrankes. Wenn z. B. ein Wert von "300" eingegeben wird und der Schrank um 8:00 Uhr morgens verriegelt wird, wird das Schloss um 13:00 Uhr entriegelt. Ein Wert von "0" bedeutet, dass die Funktion inaktiv ist.

2.4.5 Nutzungsdauer

Schränke, die für den "Freien Schrankwahl" Modus konfiguriert sind, können die Bedienung durch einen Benutzer auf eine definierte Nutzungsdauer einschränken. Für weitere Informationen siehe Abschnitt "3.6.1. Free Locker Modus (mit oder ohne die Nutzungsdauerfunktion)". Finden Sie die Nutzungsdauerfunktion hier:

Configuration > Operating mode > FreeLocker

- ▶ Wählen Sie die Art der Nutzungsdauer durch Auswahl von "Duration" (Zeitdauer) oder "Point_of_time" (Zeitpunkt) aus dem Menü "Use Time Limit".
- ▶ Definieren Sie das Zeitlimit in Minuten im Feld "Time Limit (min)".

2.4.6 Persönliche Schränke ohne Datenträger sperren

Die Funktion zum Versperren von persönlichen Schränken ohne Datenträger erlaubt es, einen Schrank nur durch Zudrücken (ohne Datenträger) automatisch zu versperren. Ein so gesperrter Schrank kann mit dem(den) Datenträger(n), der(die) an dem persönlichen Schrank berechtigt sind, geöffnet werden. Die Funktion finden Sie:

Configuration > Operating mode > PersonalLocker > PreLock Personal Locker / Pre Lock in Personal Locker mode

- ▶ Aktivieren / deaktivieren Sie die "PreLock Personal Locker" Option (bei GL7p "Pre Lock in Personal Locker mode", um die Funktion ein- / auszuschalten.

2.4.7 RF-Standards

Die Gantner Batterieschrankschlösser können mit Datenträgern arbeiten, die unterschiedliche RFID-Technologien verwenden. Welche RFID-Technologien vom Schloss unterstützt werden hängt von der Schlossvariante ab, da in den Varianten unterschiedliche RFID-Leser eingesetzt werden. Einige der Einstellungen für den Betrieb des Schlosses mit RFID-Technologien können aktiviert/deaktiviert werden und sind hier zu finden:

Configuration > Reader > RF standards

- ▶ Aktivieren / deaktivieren Sie hier die gewünschte Technologie, um die Verwendung ein- / auszuschalten.

HINWEIS! Bitte beachten Sie, dass durch die Deaktivierung von "ISO 14443" die NFC-Kommunikation deaktiviert wird und eine Konfiguration über die MoLA-App nicht mehr möglich ist.

2.4.8 MASTER Datenträger

Bis zu 10 MASTER Datenträger (in der Konfiguration auch "Master Cards" genannt) können dem Schloss zugeordnet werden, damit der Schrank unter besonderen Umständen geöffnet werden kann, z. B. wenn ein Benutzer seinen Datenträger verloren hat. Für diese Funktionalität müssen die MASTER Datenträger hier hinzugefügt werden:

Configuration > Application > Master cards > MASTER Card 1 - 10

- ▶ Geben Sie die Nummer der einzelnen, verwendeten MASTER Datenträger in dezimaler Form in die entsprechenden Felder ein.

HINWEIS! Die Schaltfläche "Lesen" im GAT ECO Lock Configurator dient dazu, den Datenträger direkt am angeschlossenen Schloss zu lesen und die Nummer in das entsprechende Feld einzutragen. Dazu müssen die RFID-Einstellungen korrekt eingestellt sein und der Datenträger muss ein gültiger MASTER- oder OPEN MASTER-Datenträger sein.



Es gibt OPEN MASTER Datenträger (nicht im GAT ECO.Basic Set enthalten). Diese Spezialdatenträger können, wie die MASTER Datenträger alle Schränke öffnen, aber nicht mehr versperren. Um einen OPEN MASTER Datenträger zu programmieren, geben Sie seine Nummer in einem der 10 "MasterCard" Feldern ein. Gesamt können 10 MASTER bzw. OPEN MASTER Datenträger konfiguriert werden.

2.4.9 Funkschnittstelle

Für Schlossvarianten mit Funkschnittstelle kann die Identifikation auch über Funk z.B. über ein Smartphone erfolgen. Eine weitere Funktion ist die Möglichkeit, den Zustand des Schlosses über einen Access Point und die eLoxx Relaxx Schrankmanagement-Software zu überwachen. Die Funkschnittstelle kann mit folgender Option eingeschaltet werden.

Configuration > Reader > BLE > General > BLE enabled

- ▶ Markieren sie die Option, wenn die Funkschnittstelle verwendet werden soll.
- ▶ In den weiteren Feldern in diesem Fenster können Sie die Funkschnittstelle konfigurieren.

2.4.10 Alarmmodus (GAT ECO.Side Lock)

Das GAT ECO.Side Lock erkennt eine unbefugte Öffnung der Schranktür, z. B. ein Aufbruch der Schranktür ohne vorherige Entriegelung. Das Schloss erzeugt ein lautes Tonsignal und die LED-Anzeige blinkt rot. Die Einstellungen für die Alarmfunktion finden Sie hier:

Configuration > Operating mode > General > Alarm Detection

- ▶ Aktivieren/deaktivieren Sie die "Alarm Detection" Option, um die Funktion ein-/auszuschalten.

2.4.11 PIN-Code Tastatur (GL7p)

Für GL7p-Varianten mit einer PIN-Code Tastatur kann die Identifikation auch über einen PIN-Code erfolgen. Die PIN-Code Eingaben muss dazu mit folgender Option eingeschaltet werden.

Configuration > Reader > KeyPad > General > KeyPad enabled

- ▶ Markieren sie die Option, wenn die PIN-Code Tastatur verwendet werden soll.
- ▶ In den weiteren Feldern in diesem Fenster können Sie die Zeit festlegen, innerhalb der ein PIN-Code eingegeben werden muss, und die erlaubte Länge des PIN-Codes einstellen. Ebenso kann definiert werden ob bei der PIN-Code Eingabe die Nutzungsdauerfunktion aktiviert sein soll.

2.4.12 Konfigurationseinstellungen

In der folgenden Tabelle sind alle verfügbaren Konfigurationsinformationen für die Gantner Batterieschrankschlösser aufgeführt.

HINWEIS! Nicht alle Einstellungen sind für alle Schlossvarianten verfügbar. Einstellungen, die nur für einen Schlosstyp spezifisch sind, sind in der Tabelle als solche gekennzeichnet.

Optionen	Beschreibung	Format	Standard
Operating mode			
General			
Operating Mode	Wählen Sie den Betriebsmodus (siehe "3.6. Betriebsmodi") des Schlosses: - FreeLocker - PersonalLocker_ProgrammingCard - PersonalLocker_ExpiryDate - FreeLocker_UniqueNumber - FreeLockerUniversal	Menü	Free Locker
Locker Number	Die Schranknummer des Schlosses. Max. Anzahl = 29.999 (BA Schlösser) bzw. 65.535 (F/ISO Schlösser)	Integer	29.999 (BA) 65.535 (F/ISO)
Beeper Mode	Ein-/Ausschalten des integrierten Piepers	Boolean	True
Alarm Detection (GAT ECO.Side Lock only)	Ein-/Ausschalten der Alarmfunktion	Boolean	False
Auto Unlock point of time [min]	Schrank zu einem definierten Zeitpunkt entriegeln (Eingabe in Minuten nach Mitternacht), "0" = inaktiv	Integer	0
Auto Unlock after locking active	Aktivieren/Deaktivieren der automatischen Entriegelung eines verschlossenen Schanks	Boolean	False
Auto Unlock after locking [min]	Der Schrank wird entriegelt, nachdem er die hier eingegebene Anzahl von Minuten gesperrt war. "0" = inaktiv.	Integer	0
FreeLocker			
Use Time Limit	Art der Schranknutzungsdauer ("3.6.1 Free Locker Modus (mit oder ohne die Nutzungsdauerfunktion)"); - "Duration" (Zeitdauer-Modus) - "Point_of_Time" (Zeitpunkt-Modus)	Menü	Duration
Time Limit [min]	Nutzungsdauer eines Schanks. Angabe in Minuten (wenn höchstwertiges Bit nicht gesetzt) oder Stunden (wenn höchstwertiges Bit gesetzt). Beispiele: Dez. Wert 1 bis 32767 -> 1 bis 32767 Minuten Dez. Wert 32768 bis 65535 -> 1 bis 32768 Stunden 0 = inaktiv	Integer	0
Time Limit Interrupt Timeout [min]	Minimale Wartezeit bis nach Ablauf der Nutzungsdauer des Schanks die nächste Nutzungsperiode beginnen kann.	Integer	60
Card Validity Date Required	Wenn dieses Feld aktiviert ist, muss ein gültiges Ablaufdatum auf den Datenträgern gesetzt sein, damit diese verwendet werden können (Standardwert 1.1.2007 ist nicht gültig)	Boolean	False
Ignore Card Validity Date	Wenn dieses Feld aktiviert ist, wird das Ablaufdatum auf den Datenträgern ignoriert.	Boolean	False
PersonalLocker			
Index Personal Locker	Index für persönliche Schränke (Mietschranke)	Integer	0
Pre Lock in Personal Locker mode	Ein-/Ausschalten der Funktion zum Sperren ohne Datenträger für persönliche Schränke (Mietschranke)	Boolean	False
Personal Locker Secure Flag / Deny assignment when locked	Ist diese Option aktiviert, ist die Übernahme eines neuen Index oder Gültigkeitsdatums von einem Datenträger in das Schloss nur bei geöffnetem Schrank möglich. Bei deaktivierter Option auch bei versperrtem Schrank (siehe "3.6.5. Personal Locker Expiry Date Modus").	Boolean	False
Last Open At Expired Date / Allow open when usage period has expired	Wenn aktiviert, kann ein Schrank nach abgelaufener Nutzungsdauer noch einmal mit dem Datenträger geöffnet werden, mit dem er gesperrt wurde (siehe "3.6.5. Personal Locker Expiry Date Modus").	Boolean	True
Write Locker Data PL ExpDate / Write locked data in PL ExpDate mode	Wenn die Option aktiviert ist, wird beim Lesen eines Datenträgers der Schlosstatus auf den Datenträger geschrieben.	Boolean	False

Reader				
RF standards				
	LEGIC Prime (nur für LEGIC Schlösser)	Wenn aktiviert, können mit dem Gerät LEGIC prime Datenträger gelesen werden	Boolean	True
	ISO15693	Wenn aktiviert, können ISO 15693 Datenträger (13,56 MHz) am Schloss gelesen werden.	Boolean	False
	ISO14443A	Wenn aktiviert, können ISO 14443 (MIFARE) Datenträger am Schloss gelesen werden. Diese Einstellung ist nicht änderbar.	Boolean	True
	INSIDE Secure	Wenn aktiviert, können Datenträger mit Inside Secure Protokoll wie z. B. HID iCLASS Datenträger am Schloss gelesen werden (nur UID/ CSN Nummer).	Boolean	False
	Sony Felica	Lese-/Schreibberechtigung auf Transpondern mit Sony Felica RF-Protokoll für den offenen Speicherbereich.	Boolean	False
	HID	Wenn aktiviert, können HID iCLASS Datenträger am Schloss gelesen werden (nur UID/ CSN Nummer).	Boolean	False
Segment configuration				
General				
	Site Key	Anlagennummer des Schlosses. Jeder Datenträger muss mit demselben Site-Key kodiert sein, um mit dem Schloss zu funktionieren.	Hex	xxx
	DESFire KeySet	Kundenspezifische DESFire AES Schlüssel, verschlüsselt. Dieser Key wird nur bei kundenspezifisch kodierten DESFire Datenträger benötigt	Hex	00000...
	Use Custom Card	Aktivieren/deaktivieren Sie die Option, eine benutzerdefinierte Karte zu verwenden (siehe folgende Einstellungen)	Boolean	False
Custom card structure				
	DataOffset	Startposition der Daten auf dem Datenträger (Byte)	Integer	0
	DataLen/Data Length	Länge der Daten auf dem Datenträger (Byte)	Integer	0
	CRCDDataStartAdr/CRC Data – Start Address	Startadresse der CRC Checksumme (Byte)	Integer	0
	CrcAdr/CRC Address	Adresse der CRC Checksumme (Byte)	Integer	0
	CrcMode/CRC Mode	Modus der CRC Checksumme: NONE, LRC, LRC_UID_BO, LEGIC_CRC8, LEGIC_CRC16	Menü	NONE
	Format	Format der Daten: BIN_LSB, BIN_MSB, BCD, ASCII	Menü	BIN_LSB
Mifare Classic				
	Sector Number	Der MIFARE Classic Sektor, in dem die Schrankinformationen auf dem Datenträger abgespeichert sind	Integer	4
	Read Key	Wählen Sie den "Read Key" (Key A oder Key B)	Menü	KEY A
	Write Key	Wählen Sie den "Write Key" (Key A oder Key B)	Menü	KEY B
Mifare DESFire				
	Read Key Num	Die Nummer des "Read Key"	Integer	1
	Write Key Num	Die Nummer des "Write Key"	Integer	2
	Application ID	ID der gewünschten DESFire-Applikation	Hex	DF8405
	Encryption Mode	Wählen Sie die Art des Verschlüsselungsmodus	Menü	AES
	File Number	DESFire Locker File, in welchem die Schrankinformationen gespeichert sind	Integer	1
	File Comm Mode	Dateikommunikationsmodus: "Plain", "Maced", "Enciphered"	Menü	ENCIPHERED
	FileType	Dateiart: "Standard", "Backup"	Menü	BACKUP
	File Data Offset	Daten-Offset im DESFire Schrank-File	Integer	0
ISO15693				
	General Block Num	Das Segment, in dem allgemeine Daten gespeichert sind.	Integer	13
	Certificate Block Num	Das Segment, in dem Zertifikatdaten gespeichert sind.	Integer	15
	Locker Block Num	Das Segment, in dem Schrankdaten gespeichert sind.	Integer	19
LEGIC prime (nur für LEGIC Schlösser)				
	SearchStr	LEGIC prime Stamp. Aufbau wie folgt: 1. ID: Gantner Standard = 1A2200 2. FID: Standard = 9999 3. Segment-ID: Standard = 03	Text	1A2200 999903
	Search String Length	Länge des Stamps	Integer	6
	Legic Locker	Wählen Sie hier die LEGIC-Schranknummer (1 oder 2) in den auf dem Datenträger kodierten Schrankinformationen	Menü	Locker1

	LEGIC advant (nur für LEGIC Schlösser)	Einstellungen für LEGIC advant Datenträger		
	Stamp	Wert für den Stamp für LEGIC advant. Aufbau wie folgt: 1. ID: Gantner Standard = 1A24 2. FID: Standard = 00009999 3. Segment-ID: Standard = 0008 4. 00000000	Text	1A240000 99990008
	Stamp String Length	Länge des LEGIC advant Stamp in Byte	Integer	8
Gantner.Connect				
	File ID	ID-Nummer für Gantner.Connect.	Integer	1
Basic Set configuration				
General				
	SiteKey	Anlagennummer des verwendeten Basic Sets.	Hex	xxx
	DESFire KeySet	Kundenspezifische DESFire AES Schlüssel, verschlüsselt. Dieser Key wird nur bei kundenspezifisch kodierten DESFire Datenträger benötigt	Hex	
	Use user card settings	Einstellungen der allgemein definierten Datenträger verwenden (siehe "Segment configuration"). Ist diese Funktion ausgewählt werden die restlichen Basic Set Einstellungen nicht beachtet!	Boolean	True
BLE (nur bei Schlossvarianten mit Funkschnittstelle)				
General				
	BLE enabled	Option zum ein- und ausschalten der Funkschnittstelle	Boolean	False
	KeySet BLE / BLE KeySet	Kundenspezifischer Schlüssel für die Funkschnittstelle. Gantner Standard = 0.	Hex	
	BLE advertise timeout in idle mode	Dauer wie lange die Informationspakete (BLE Advertise) im idle Mode (Tiefschlafmode des Schlosses) versendet werden. Der Idle-Mode beginnt nach Ablauf des Activation-Mode. Bei Eingabe von "0" ist der Idle-Mode unbegrenzt aktiv.	Integer	0
	BLE pulse period in idle mode	Abstand in welchem die Informationspakete (BLE Advertise) im Idle-Mode versendet werden. Eingabe in 100 ms (z. B. 600 = 1 Minute). Jeder Puls benötigt Energie, deshalb sollte die Periode je nach Anwendungsfall so groß gewählt werden, dass eine Erkennung des Informationspakets noch gut möglich ist.	Integer	100
	BLE advertising timeout when activated	Dauer wie lange die Informationspakete (BLE Advertise) im Activation-Mode (nach Betätigung des Tasters) versendet werden. Eingabe in 100 ms (z. B. 600 = 1 Min.). Nach Ablauf des Activation-Mode startet der Idle-Modus. Bei Eingaben von "0" ist der Arbeitsmodus unbegrenzt aktiv und der Idle-Modus wird nicht verwendet.	Integer	150
	BLE pulse period when activated	Abstand in welchem die Informationspakete (BLE Advertise) im Arbeitsmodus (Betätigungen) versendet werden. Eingabe in 100 ms (z. B. 600 = 1 Minute). Jeder Puls benötigt Energie, deshalb sollte die Periode so gewählt werden, dass im Arbeitsmodus eine Erkennung des Funk-signals schnell möglich ist.	Integer	5
	BLE PreLock Timeout	Zeitraum (in Sekunden) zum Versperren des Schlosses nach Empfang des Verriegelungsbefehls über die Funkschnittstelle. Eingabe in Sekunden.	Integer	10
	BLE Advertising Format	Typ, der für die BLE Advertise Daten verwendet wird. Für das Vernetzen per BLE Gateways wird der Type 1 benötigt.	Menü	TYPE1
KeyPad (nur für GL7p-Varianten)				
General				
	KeyPad enabled	Mit Setzen dieser Option aktivieren Sie die PIN-Code Eingabe (bei GL7p.13xx und GL7p.33xx).	Boolean	True
	PIN code timeout	Max. Eingabezeit zwischen 2 Stellen des PIN-Codes. Wenn in dieser Zeit kein weiterer Tastendruck erfolgt, und auch nicht mit (✓) oder Taster bestätigt wird, wird die Eingabe abgebrochen. Eingabe in 100 ms (z. B. Standardwert 40 = 4 Sekunden).	Integer	40
	Minimum PIN length	Minimal notwendige PIN-Code Länge	Integer	4
	Maximum PIN length	Maximal erlaubte PIN-Code Länge	Integer	7
	Activate PIN code UseTimeLimit	Ist diese Option gesetzt, wird für die PIN-Code Eingabe auch, analog zur Bedienung mit Datenträgern, die Nutzungsdauer verwendet (siehe "3.6.1. Free Locker Modus (mit oder ohne die Nutzungsdauerfunktion)").	Boolean	False

Application				
General				
Legacy BasicSet Coding	Datenträger im Basic Set sind für ein Vorgängersystem kodiert (bisherige Kodierung).	Boolean	False	
Master cards				
MASTER Card 1.. 10	Die Felder, in den die Nummern der MASTER oder OPEN MASTER Datenträger 1-10 hinzugefügt werden.	Integer		
License				
License Certificate Check	Wenn hier "installed" angezeigt wird, kann die Zertifikatsprüfung ein-/ausgeschaltet werden.	Info	installed	
Certificate Check enabled	Zertifikatsprüfung für Datenträger ein- oder ausschalten.	Boolean	False	
Read only parameter				
Production				
Produktionsspezifische Informationen				
Article Number	Artikelnummer des Schlosses	Integer		
Serial Number	Seriennummer des Schlosses	Integer		
Manufacturer code	Herstellernummer des Schlosses	Integer		
ProductionYear	Baujahr des Schlosses	Integer		
ProductionWeek	Kalenderwoche, an der das Schloss produziert wurde	Integer		
Hardware Unique Number	Eindeutige Identifikationsnummer der Hardware	Integer		
Device Type	Typnummer des Schlosses			
Hardware Version	Hardware-Version des Schlosses	Integer		
Bootloader Version	Bootloader-Version des Schlosses	Integer		
Firmware Version	Firmware-Version des Schlosses	Integer		
Lock Engine Version	Version der Schlosslogik	Integer		
Electronic Assembly ID	Identifikationsnummer der Baugruppe	Integer		
Internal				
Interne Daten für Servicezwecke				
Antenna matching	Antennenabstimmung	Integer		
CNT Activation	Anzahl Betätigungen des Tasters seit dem Rücksetzen des Zählers	Integer		
CNT Locking	Anzahl gültiger Verriegelungen (mit Datenträger oder PIN) seit dem Rücksetzen des Zählers	Integer		
CNT Activation ABS	Gesamte Anzahl Betätigungen des Tasters	Integer		
CNT Locking ABS	Gesamte Anzahl Verriegelungen (mit Datenträger oder PIN)	Integer		
Temp. int.	Temperatur im Schloss in °C	Integer		
BV	Information für Servicetechniker			
TL	Information für Servicetechniker			
MC	Information für Servicetechniker			
BM	Information für Servicetechniker			
ReaderChip				
FW / Reader Firmware Version	Firmware der RFID Leserelektronik			
Telemetry				
Statusinformationen über die Bedienung des Schlosses				
Duration Locked [min.]	Zähler, der anzeigt, wie lange das Schloss insgesamt versperrt war (in Minuten)	Integer		
CNT activations last locking	Anzahl der Betätigungen des Tasters seit dem letzten Versperren des Schlosses	Integer		
CNT door released while locking	Anzahl der abgebrochenen Schließvorgänge.	Integer		
CNT write on card failed 1	Anzahl Fehler beim Schreiben auf den Datenträger, erster Versuch	Integer		
CNT write on card failed 2	Anzahl Fehler beim Schreiben auf den Datenträger, zweiter Versuch	Integer		
CNT write on card failed card removed	Anzahl Fehler beim Schreiben auf den Datenträger, weil der Datenträger zu früh vom Lesefeld entfernt wurde	Integer		
BLE				
BLE Module / FW Version	Firmware der Funkschnittstellenelektronik	Integer		
MAC	MAC network address of the lock (BLE Module)	Hex		
BatteryMgt				
Settings				
Batt Idle MA	Information für Servicetechniker	Integer		
Batt Idle	Information für Servicetechniker	Integer		
Supply Reg OFF	Information für Servicetechniker	Integer		

Tabelle 2.1 – Konfigurationseinstellungen

3 BEDIENUNG

Funk-HF-Exposition

Die Benutzer müssen einen Abstand von mindestens 20 cm zum Schloss einhalten, außer während der Identifizierungs- und Bedienprozesse am Schloss (z. B. Eingabe des PIN-Codes), der wie in diesem Handbuch beschrieben durchgeführt werden muss.

3.1 Zielgruppe

Dieses Kapitel enthält Informationen für die Techniker, die für die Inbetriebnahme des Schlosses und für die Durchführung von Servicearbeiten bei Betriebsstörungen zuständig sind.

3.2 Allgemein

Die Gantner Batterieschrankschlösser können in den Betriebsarten "Free Locker" oder "Personal Locker" betrieben werden. Bei Free Locker kann der Kunde einen beliebigen Schrank wählen, bei Personal Locker wird dem Kunden ein bestimmter Schrank zugeteilt, den nur er benutzen kann.

Werden in einer Anlage Personal Locker und Free Locker Schränke gemeinsam verwendet, wird empfohlen, die Schranknummern aller Schlösser der Anlage eindeutig zu vergeben. Es sollte niemals dieselbe Schranknummer sowohl für einen Personal Locker als auch für einen Free Locker verwendet werden.

Um das Schloss zu bedienen (z. B. um einen Schrank zu versperren oder öffnen), muss sich der Benutzer am Schloss mit seinem RFID-Datenträger oder per PIN-Code (nur GL7p) identifizieren. Um Batterieladung zu sparen, ist das Schloss im Normalzustand deaktiviert und die Schlosselektronik muss aktiviert werden, bevor eine Identifizierung oder Bedienung erfolgen kann. Beim GL7p und GAT ECO.Lock geschieht dies durch Drücken der Schlosstaste mit Hilfe des Datenträgers. Beim GAT ECO.Side Lock muss die Schranktür eingedrückt werden, während der Datenträger vor die Schloss-LED gehalten wird. Durch diesen Vorgang wird der RFID-Leser aktiviert und der Datenträger wird ausgelesen.

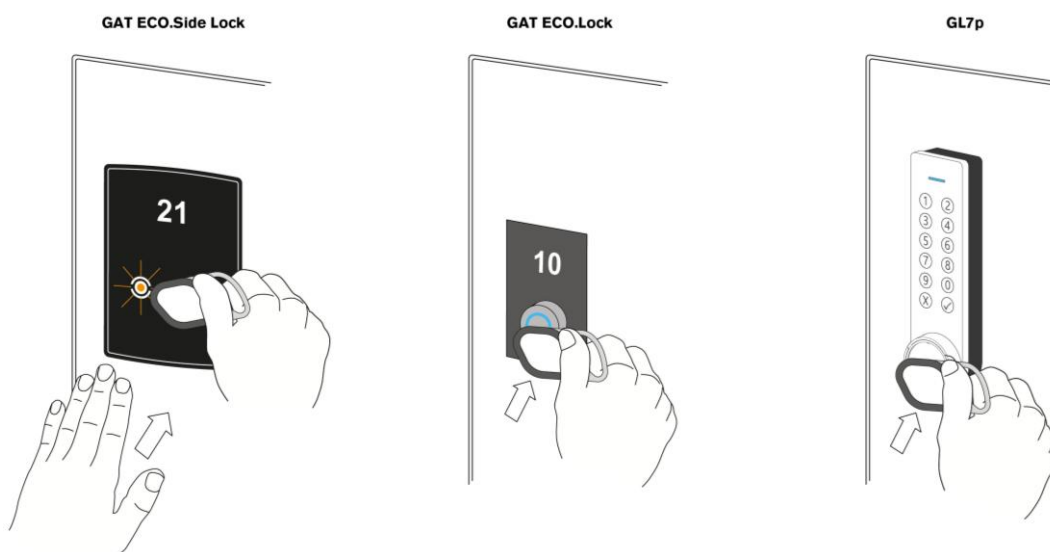


Bild 3.1 – Aktivieren der Elektronik und des RFID-Lesers des Schlosses

3.3 PIN-Code Bedienung (GL7p)

Bei den GL7p-Schlössern mit Tastatur (GL7p.1xxx und GL7p.3xxx) kann die Bedienung des Schlosses, d.h. das Ver- und Entriegeln, anstatt mittels Datenträgers auch durch Eingabe eines PIN-Codes erfolgen.



Siehe Abschnitt "2.4.11. PIN-Code Tastatur (GL7p)" für Informationen, wie Sie die Tastatur für den PIN-Code-Betrieb aktivieren.

Nach Eingabe des PIN-Codes muss dieser durch Drücken der Taste "✓" oder durch Drücken des Druckknopfes bestätigt werden. Ein RFID-Datenträger ist dann nicht erforderlich. Ein eingegebener PIN-Code kann durch Drücken der "X" Taste gelöscht werden.

Die Länge des PIN-Codes ist konfigurierbar (siehe "2.4.12. Konfigurationseinstellungen"). Damit die persönlichen PIN-Codes geschützt bleiben, werden die ins Schloss eingegebenen PIN-Codes nicht in den Schlossbuchungen protokolliert und können nicht ausgelesen werden.

3.4 Alarmbehandlung (GAT ECO.Side Lock)

Das GAT ECO.Side Lock kann erkennen, ob eine versperrte Schranktür mit Gewalt unbefugt geöffnet wird (ohne vorige Entriegelung). Um zuständiges Personal über einen solchen Aufbruchsversuch zu alarmieren, wird ein lautes Alarmsignal ausgegeben und die LED blinkt rot.



Bei Auslieferung ist die Alarmfunktion deaktiviert. Siehe Abschnitt "2.4.10. Alarmmodus (GAT ECO.Side Lock)" für weitere Informationen, wie die Funktion aktiviert werden kann.

Um einen Schrankalarm zu deaktivieren, gehen Sie wie folgt vor:

- ▶ Drücken Sie die Schranktür zu und halten Sie sie gedrückt.
- ▶ Halten Sie einen MASTER Datenträger auf das RFID-Lesefeld (siehe Abschnitt "3.8.1. MASTER Datenträger").
 - Der Alarmton wird deaktiviert und die LED hört auf zu blinken.
- ▶ Wenn die Schranktür noch geschlossen ist, drücken Sie die Schranktür mit einer Hand und halten Sie einen MASTER Datenträger oder den Datenträger, der den Schrank zuvor versperrt hatte, auf das RFID-Lesefeld.
 - Die Schranktür öffnet sich.

HINWEIS! Das GAT ECO.Side Lock, das Boltset und der Türbügel müssen nach einem Einbruchsversuch ersetzt werden.

3.5 Automatischer Antennenabgleich (GAT ECO.Side Lock)

Die Antenne des GAT ECO.Side Lock kann kalibriert werden, um die optimale Lesereichweite für die RFID-Datenträger sicherzustellen. Um diesen Abgleich durchzuführen ist das Schloss mit einer automatischen Antennenabgleichfunktion ausgestattet, die mit dem SERVICE Datenträger oder über die Konfigurationssoftware aktiviert werden kann.

3.5.1 Antennenabgleich mit dem SERVICE Datenträger

Der SERVICE Datenträger ist im GAT ECO.Basic Set enthalten (siehe "3.7. GAT ECO.Basic Set"). Gehen Sie folgendermaßen vor, um den Antennenabgleich durchzuführen.

- ▶ Schließen Sie die Schranktür und halten Sie sie zugedrückt.
- ▶ Halten Sie den SERVICE Datenträger auf das RFID-Lesefeld. Entfernen Sie den Datenträger unmittelbar nach Aktivierung (Start) des Antennenabgleichs.
 - Der Antennenabgleichprozess beginnt und die Status-LED blinkt für 5 Sekunden rot. Der Vorgang ist abgeschlossen, wenn die LED für 1 Sekunde grün blinkt und das Schloss ein Tonsignal ausgibt.



Die Antennenabgleichfunktion kann auch aktiviert werden, wenn die Schranktür verriegelt ist.

3.5.2 Antennenabgleich über GAT ECO Lock Configurator

- ▶ Klicken Sie in der GAT ECO Lock Configurator Software in der Registerkarte "Remote" auf "Adjust Antenna".
 - Der Antennenabgleichprozess beginnt und wird automatisch durchgeführt.

3.6 Betriebsmodi



In der folgenden Anleitung wird der Vorgang des "Aktivierens" des Schlosses allgemein als "aktivieren" beschrieben. Dieser Vorgang ist für alle Schlossvarianten etwas unterschiedlich, siehe Bild 3.1.

Es sind folgende Betriebsmodi möglich:

"Free Locker" (früher auch als "Freie Schrankwahl" bezeichnet)

- Free Locker - mit oder ohne Nutzungsdauerfunktion (Standard)
- Free Locker Universal

HINWEIS! Der Modus "Free Locker Universal" ist nur mit MIFARE-Datenträgern verfügbar.

- Free Locker Unique Number

"Personal Locker" (früher auch als "Persönliche Schränke" bezeichnet)

- Personal Locker Programming Card
- Personal Locker Expiry Date

Voraussetzungen für LEGIC prime, LEGIC advant, MIFARE, ISO 15693 und HID iClass Datenträger

Alle MIFARE und ISO 15693 Datenträgern, die in den verschiedenen Betriebsmodi verwendet werden, müssen die folgenden Anforderungen erfüllen.

Betriebsmodus	Anforderungen für Datenträger
Free Locker	Datenträger muss entsprechend mit den Gantner Schrankinformationen kodiert sein.
Free Locker Universal	Der eingestellte Datenbereich der MIFARE-Datenträger muss unbenutzt sein (mit lauter Nullen kodiert sein) und die Schreib- / Leserechte müssen vorhanden und konfiguriert sein.
Free Locker Unique Number	Die Datenträger müssen nicht kodiert sein. Alle LEGIC, MIFARE, ISO 15693 und HID iClass Datenträger sind einsetzbar, sofern keine Random UID vorhanden ist.
Personal Locker Programming Card	Die Datenträger müssen nicht kodiert sein. Alle LEGIC, MIFARE, ISO 15693 und HID iClass Datenträger sind einsetzbar, sofern keine Random UID vorhanden ist.
Personal Locker Expiry Date	Datenträger muss entsprechend mit den Gantner Schrankinformationen kodiert sein.

Tabelle 3.1 – Anforderungen an Datenträger

3.6.1 Free Locker Modus (mit oder ohne die Nutzungsdauerfunktion)

Bei der Betriebsart Free Locker hat der Kunde die Möglichkeit, sich einen freien Schrank auszusuchen und diesen mit seinem Datenträger zu verschließen. Nach Verschließen des Schrankes kann der Benutzer innerhalb der gleichen Schrankgruppe keine weiteren Schränke belegen. Erst nach dem Öffnen desselben Schrankes kann der Kunde wieder einen anderen Schrank in dieser Schrankgruppe benutzen.

Schrankgruppen werden verwendet, um die Schlösser innerhalb einer Anlage in bestimmte funktionelle Blöcke wie Garderobenschränke, Wertfächer etc. zu unterteilen. Jede Schrankgruppe verwendet eine unterschiedliche Sektornummer auf den Datenträgern. Dadurch können, abhängig vom Speicherplatz auf dem Datenträger, zwei oder mehr Schränke in verschiedenen Gruppen mit demselben Datenträger benutzt werden.

Bei Datenträgern, auf denen ein Ablaufdatum gesetzt wurde, wird dieses Datum im Schloss geprüft. Ist dieses Datum überschritten, kann der Schrank nicht benutzt werden.

HINWEIS! Das Schloss führt die Sommer-/Winterzeitschaltung nicht automatisch durch. Dies muss beim Schreiben des Gültigkeits- bzw. Ablaufdatums berücksichtigt werden.

Verriegeln und Entriegeln von Schränken mit Datenträger

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen.
 - a) Gültiger Datenträger: Die LED leuchtet kurz blau und dann grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt.
 - b) Ungültiger Datenträger: Die LED leuchtet kurz blau und dann rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet. Möglicher Grund dafür sind:
 - Mit dem verwendeten Datenträger wurde schon ein anderer Schrank versperrt. Dieser muss dann zuerst wieder geöffnet werden.
- ▶ Kontrollieren Sie beim Versperren des Schrankes durch Ziehen der Schranktür, ob diese versperrt ist.

Verriegeln und Entriegeln von Schränken mit PIN-Code (nur GL7p)

- ▶ Geben Sie ihren PIN-Code ein.

HINWEIS! Die Länge des PIN-Codes kann in der Konfiguration definiert werden.
- ▶ Drücken Sie zur Bestätigung des PIN-Codes die OK-Taste (✓) und anschließend die Schlosstaste oder drücken Sie einfach direkt die Schlosstaste.
 - Der PIN-Code wird überprüft.
 - c) Gültiger PIN-Code: Die LED leuchtet kurz grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt.
 - d) Ungültiger PIN-Code: Die LED leuchtet kurz rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet.
- ▶ Kontrollieren Sie beim Versperren des Schrankes durch Ziehen der Schranktür, ob diese versperrt ist.

Nutzungsdauerfunktion

Im Modus Free Locker besteht weiters die Möglichkeit, jedem Datenträger eine limitierte Nutzungsdauer zu geben. Wenn mit solch einem Datenträger ein Schrank mit dieser Funktion versperrt wird, wird der aktuelle Zeitpunkt auf den Datenträger geschrieben und diese Zeit wird beim späteren Öffnen des Schrankes kontrolliert. Mit PIN-Code Eingabe ist diese Funktion auch möglich. Dabei ist zu beachten, dass jede Eingabe eines neuen PINs die maximale Nutzungszeit wieder neu startet.

Ein Schrank kann während der gültigen Nutzungsdauer so oft wie gewünscht ver- und entriegelt werden. Ist die definierte Nutzungsdauer überschritten, kann der Schrank mit dem Datenträger nicht mehr geöffnet werden. In

diesem Fall muss der Anwender den Datenträger an zentraler Stelle neu codieren lassen. Dies ist z. B. an einem GT7 Terminal mit G7 Info App möglich. Bei Überschreiten der maximalen Nutzungsdauer bei Nutzung eines PINs ist das Schloss mit einem gültigen MASTER Datenträger zu öffnen.

HINWEIS! Für die Nutzungsdauerfunktion müssen die Datenträger entsprechend kodiert werden (setzen des entsprechenden Config-Bits auf dem Datenträger). Diese Funktion ist bei LEGIC prime Datenträgern nicht verfügbar. Beim Einsatz mit einem PIN-Code ist die Nutzungsdauerfunktion in der Konfiguration separat zu aktivieren (siehe Abschnitt "2.4.11. PIN-Code Tastatur (GL7p)"). Das Schloss muss zusätzlich für die Nutzungsdauerfunktion konfiguriert werden (siehe Abschnitt "2.4.5. Nutzungsdauer"). Es gibt zwei Konfigurationsoptionen für die Funktion:

> Absolute Nutzungsdauer ("Zeitdauer" bzw. "Duration" Funktion)

In diesem Modus wird eine Nutzungsdauer (Angabe abhängig vom Parameter "Time limit" in Minuten oder Stunden, siehe "2.4.12. Konfigurationseinstellungen") konfiguriert. Versperrt ein Datenträger einen Schrank, muss der Benutzer den Schrank innerhalb dieser Zeitdauer wieder öffnen. Die Zeitdauer beginnt ab dem Versperren des Schanks.

Beispiel:

Die Nutzungsdauer wurde auf 360 Minuten (3 Stunden) eingestellt (Parameter Time Limit [min]). Wird der Schrank um 10:00 Uhr versperrt, kann er bis 13:00 Uhr wieder geöffnet werden. Wird der Schrank um 14:00 Uhr versperrt, kann er bis 17:00 Uhr geöffnet werden. Die Nutzungsdauer wird zurückgesetzt, wenn der Schrank länger als 60 Minuten geöffnet ist (Parameter Time Limit Interrupt Timeout [min]). Wird ein beliebiger Schrank mit aktiver Duration Funktion innerhalb der definierten Interrupt Timeout wieder versperrt läuft die zuvor aktive Nutzungsdauer weiter.

Kann ein Schrank auf Grund der überschrittenen Nutzungsdauer nicht mehr geöffnet werden muss der Anwender den Datenträger an zentraler Stelle neu freigeben lassen, z. B. an einem GT7 Terminal mit G7 Info App.

> Nutzung bis zu einem bestimmten Zeitpunkt nach Mitternacht ("Zeitpunkt" bzw. "Point of Time" Funktion)

In diesem Modus wird eine Zeit konfiguriert, bis zu der der Schrank jeden Tag verwendet werden kann. Versperrt ein Datenträger einen Schrank, muss der Benutzer den Schrank vor diesem Zeitpunkt wieder öffnen. Die Zeitdauer beginnt jeweils ab der konfigurierten Zeit nach Mitternacht.

Beispiel:

Die Zeit wird auf 120 Minuten eingestellt. Da die Berechnung ab Mitternacht beginnt (unabhängig davon, wann der Schrank versperrt wurde), kann der Schrank bis 2:00 Uhr am folgenden Tag benutzt werden. Wird der Schrank z. B. um 1:00 Uhr versperrt, kann er bis 2:00 Uhr am folgenden Tag geöffnet werden. Bleibt der Schrank länger verschlossen, kann der Schrank mit dem Datenträger nicht mehr geöffnet werden. In diesem Fall muss der Anwender den Datenträger an zentraler Stelle neu freigeben lassen, z. B. an einem GT7 Terminal mit G7 Info App.

Verriegeln und Entriegeln von Schränken mit Datenträger

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen.
 - a) Gültiger Datenträger: Die LED leuchtet kurz blau und dann grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt. Die Zeit auf dem Datenträger wird überprüft, und die aktuelle Zeit auf den Datenträger geschrieben.
 - b) Ungültiger Datenträger: Die LED leuchtet kurz blau und dann rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet. Möglicher Grund dafür sind:
 - Mit dem verwendeten Datenträger wurde schon ein anderer Schrank versperrt. Dieser muss dann zuerst wieder geöffnet werden.
 - Die Nutzungsdauer ist überschritten und der Schrank kann nicht mehr geöffnet werden. In diesem Fall muss der Datenträger an einer zentralen Station zurückgesetzt werden.
- ▶ Kontrollieren Sie beim Versperren des Schanks durch Ziehen der Schranktür, ob diese versperrt ist.

3.6.2 Free Locker Universal Modus

Der Betriebsmodus Free Locker Universal unterscheidet sich vom Standard Modus Free Locker in folgenden Punkten:

- > Der Free Locker Universal Mode (Freie Schrankwahl Universal Modus) erlaubt die Verwendung von Datenträgern, die nicht mit den Gantner Schrankinformationen kodiert wurden.
- > Kein Gültigkeitsdatum im Free Locker Universal Modus.
- > Die Nutzungsdauerfunktion ist im Free Locker Universal Modus nicht möglich.
- > Für die Datenträger müssen folgende zwei Punkte beachtet werden:
 1. Sie müssen eine MIFARE Classic oder MIFARE DESFire Technologie verwenden.
 2. Der Schranksektor bzw. die Datei muss unbenutzt bzw. "leer", d.h. mit lauter Nullen codiert sein.
 3. Die Access-Keys müssen stimmen.

ACHTUNG! Bei Aktivierung des "Free Locker Universal Modus" und gleichzeitiger Verwendung von kodierten Datenträgern werden beim Öffnen des Schanks alle Daten von dem eingestellten Datenträgerbereich gelöscht! Diese Datenträger können in Folge bei Schlössern im "Free Locker" oder "Personal Locker Expiry Date" Mode nicht mehr genutzt werden. Um diese Datenträger wieder nutzen zu können müssen die entsprechenden Datenbereiche neu kodiert werden!

Verriegeln und Entriegeln von Schränken mit Datenträger

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen.
 - a) Gültiger Datenträger: Die LED leuchtet kurz blau und dann grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt.
 - b) Ungültiger Datenträger: Die LED leuchtet kurz blau und dann rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet.
- ▶ Kontrollieren Sie beim Versperren des Schanks durch Ziehen der Schranktür, ob diese versperrt ist.

3.6.3 Free Locker Unique Number Modus

Dieser Betriebsmodus unterscheidet sich vom Standard Modus "Free Locker" in folgenden Punkten:

- > Alle LEGIC, MIFARE, HID iClass und ISO 15693 Datenträger können mit dem Schloss verwendet werden, sofern sie keine zufälligen Unikatsnummern (Random UID) verwenden.
- > Auf dem Datenträger muss sich kein Gantner-Schranksegment befinden.
- > Beim Schließen eines Schanks mit einem Datenträger wird die Schrankbenutzung nicht auf den Datenträger geschrieben.
- > Jeder Datenträger kann zu jeder Zeit eine beliebige Anzahl von Schränken benutzen (versperren).

Verriegeln und Entriegeln von Schränken mit Datenträger

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen.
 - a) Gültiger Datenträger: Die LED leuchtet kurz blau und dann grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt.
 - b) Ungültiger Datenträger: Die LED leuchtet kurz blau und dann rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet.
- ▶ Kontrollieren Sie beim Versperren des Schanks durch Ziehen der Schranktür, ob diese versperrt ist.

Verriegeln und Entriegeln von Schränken mit PIN-Code (nur GL7p)

- ▶ Geben Sie ihren PIN-Code ein.
HINWEIS! Die Länge des PIN-Codes kann in der Konfiguration definiert werden.
- ▶ Drücken Sie zur Bestätigung des PIN-Codes die OK-Taste (✓) und anschließend die Schlosstaste oder drücken Sie einfach direkt die Schlosstaste.
 - Der PIN-Code wird überprüft.
 - a) Gültiger PIN-Code: Die LED leuchtet kurz grün auf und die Aktion (verriegeln, entriegeln) wird durchgeführt.
 - b) Ungültiger PIN-Code oder Nutzungszeit abgelaufen: Die LED leuchtet kurz rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet.
- ▶ Kontrollieren Sie beim Versperren des Schrankes durch Ziehen der Schranktür, ob diese versperrt ist.

3.6.4 Personal Locker Programming Card Modus

Beim Betriebsmodus Personal Locker Programming Card können pro Schloss bis zu 32 Datenträger oder 32 PIN-Codes (nur GL7p) berechtigt werden. Die max. 32 Berechtigungen können mit dem Schrank beliebig oft verwendet werden und teilen sich den gleichen Berechtigungszugang, z.B. für die Verwendung als Familienkarte.

Die Berechtigungen werden dem Schloss mit einem PROGRAM Datenträger eingelernt (Teil des GAT ECO.Basic Set, siehe Abschnitt "3.7. GAT ECO.Basic Set").

Berechtigten von Datenträgern

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem PROGRAM Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen und die LED leuchtet kurz grün auf.
- ▶ Das Schloss wechselt in den Programmiermodus.
 - Die LED blinkt bis zum Entfernen des PROGRAM Datenträgers rot. Sobald der PROGRAM Datenträger entfernt wurde, blinkt die LED rot/grün und das Schloss ist bereit für die Programmierung von Datenträgern.
- ▶ Halten Sie den zu berechtigenden Datenträger innerhalb von 5 Sekunden vor das Schloss (das Schloss muss nicht aktiviert sein).
 - a) Erfolgreiche Berechtigung: Die LED leuchtet 3 Sekunden lang grün auf. Wird der Datenträger entfernt fängt die LED wieder rot und grün an zu blinken und es kann der nächste Datenträger berechtigt werden. Dieser Vorgang kann solange wiederholt werden, bis alle gewünschten Datenträger berechtigt sind.
 - b) Fehlgeschlagene Berechtigung: Die LED leuchtet rot auf. Ein möglicher Grund dafür ist, dass der Datenträger nicht korrekt gelesen werden konnte (z. B. weil der Datenträger beschädigt ist).
- ▶ Sie können den letzten Schritt mit verschiedenen Datenträgern wiederholen, um diese Datenträger direkt hintereinander einzuprogrammieren. Dazu muss jeder Datenträger innerhalb von 5 Sekunden nach Entfernen des vorigen Datenträgers vom Schloss gelesen werden. Wenn Sie länger als 5 Sekunden warten, wird der Einlernvorgang beendet und die bis zu diesem Zeitpunkt gelesenen Datenträger gespeichert.

Berechtigten von PIN-Codes (nur GL7p)

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem PROGRAM Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen und die LED leuchtet kurz grün auf.
- ▶ Das Schloss wechselt in den Programmiermodus.
 - Die LED blinkt bis zum Entfernen des PROGRAM Datenträgers rot. Sobald der PROGRAM Datenträger entfernt wurde, blinkt die LED rot/grün und das Schloss ist bereit für die Programmierung von Datenträgern.
- ▶ Drücken Sie zur Bestätigung des PIN-Codes die OK-Taste (✓) und anschließend die Schlosstaste oder drücken Sie einfach direkt die Schlosstaste.
 - a) Erfolgreiche Berechtigung: Die LED leuchtet 3 Sekunden lang grün auf. Danach fängt die LED wieder rot und grün an zu blinken und es kann der nächste PIN-Code berechtigt werden. Dieser Vorgang kann solange wiederholt werden, bis alle gewünschten PIN-Codes berechtigt sind.
 - b) Fehlgeschlagene Berechtigung: Die LED leuchtet dreimal rot auf. Ein möglicher Grund dafür ist, dass der PIN-Code nicht korrekt gelesen werden konnte, z. B. weil der PIN-Code zu kurz oder zu lang war oder weil ein ungültiger PIN-Code eingegeben wurde.
- ▶ Sie können den letzten Schritt mit verschiedenen PIN-Codes wiederholen, um diese direkt hintereinander einzuprogrammieren. Dazu muss die Eingabe eines PIN-Codes innerhalb von 5 Sekunden nach Bestätigung des vorigen PIN-Codes gestartet werden. Wenn Sie länger als 5 Sekunden warten, wird der Einlernvorgang beendet und die bis zu diesem Zeitpunkt gelesenen PIN-Codes gespeichert.

Sperrern von Datenträgern oder PIN-Codes (= Berechtigungen löschen)

Es können nur alle Berechtigungen gesamthaft im Schloss gelöscht werden.

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem PROGRAM Datenträger.
 - Die Informationen auf dem Datenträger werden gelesen und die LED leuchtet kurz grün auf.
- ▶ Das Schloss wechselt in den Programmiermodus.
 - Die LED blinkt bis zum Entfernen des PROGRAM Datenträgers rot. Sobald der PROGRAM Datenträger entfernt wurde, blinkt die LED rot/grün und das Schloss ist bereit für den nächsten Schritt.
- ▶ Halten Sie innerhalb von 5 Sekunden den PROGRAM Datenträger für ca. 1 Sekunde vor das Schloss.
- ▶ Bei erfolgreich durchgeführter Aktion blinkt die LED 3 mal rot und es werden 2 Signaltöne ausgegeben. Das Schloss schaltet sich danach wieder aus.
 - Alle Datenträger und PIN-Codes sind nun im Schloss gelöscht und haben darum keine Berechtigung mehr, das Schloss auf- oder zuzusperren.

Übertragen von Berechtigungen auf ein neues Schloss

Wenn ein Schloss, das im Modus Personal Locker Programming Card betrieben wird, durch ein neues Schloss ersetzt wird, können die bestehenden Einstellungen und Datenträgerberechtigungen im GAT ECO Lock Configurator wie folgt auf das neue Schloss übertragen werden.

- ▶ Bevor Sie das zu ersetzende Schloss an den PC anschließen, wählen Sie im GAT ECO Lock Configurator die Option "Copy with Personal Locker Cards".

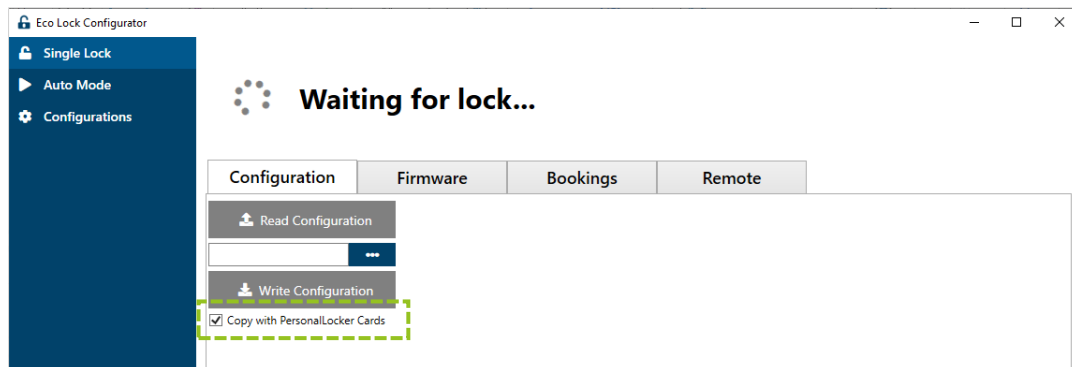


Bild 3.2 – Option "Copy with Personal Locker Cards"

- ▶ Schließen Sie das zu ersetzende Schloss an den PC an und wählen Sie "Read Configuration".
 - Die Konfiguration des Schlosses sowie die gespeicherten Datenträger werden ausgelesen.
- ▶ Öffnen Sie über die Seitenleiste die Seite "Configurations" des GAT ECO Lock Configurator.

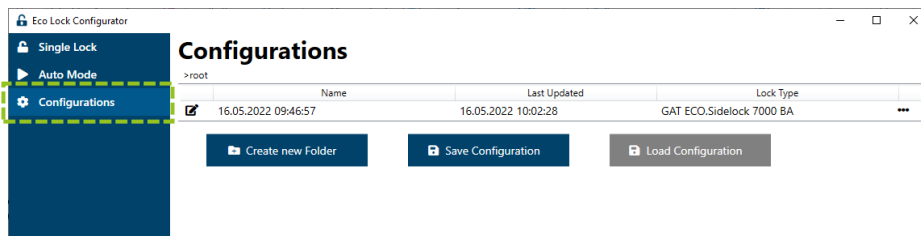


Bild 3.3 – Seite "Configurations"

- ▶ Hier können Sie die Schlosskonfiguration über die Schaltfläche "Save Configuration" speichern.
- ▶ Stecken Sie das zu ersetzende Schloss am PC ab und schließen Sie nun das neue Schloss an den PC.
- ▶ Laden Sie die Konfigurationsdatei über die Schaltfläche "Load Configuration" in das Schloss.



Weitere Informationen finden Sie im Handbuch des GAT ECO Lock Configurator.

3.6.5 Personal Locker Expiry Date Modus



Informationen für GL7p-Schlösser:

Da mit PIN-Codes kein Gültigkeitsdatum gespeichert werden kann, ist dieser Modus beim GL7p nur mit RFID-Datenträgern und nicht mit PIN-Code-Betrieb möglich.

Information für LEGIC prime Systeme:

Bei Systemen mit LEGIC prime entfällt der Index Wert bei Datenträgern.

Der Kunde erhält einen Datenträger mit einer kodierten Gantner Schrankinformationen. Auf dem berechtigten Datenträger werden die persönliche Schranknummer des Kunden sowie das Ablaufdatum ("gültig von" und "gültig bis") geschrieben. Außerdem wird ein Indexwert in den Schrankinformationen geschrieben. Das "gültig von" Datum muss immer gültig sein, d.h. neuer oder gleich wie das Datum im benutzten Schloss.

Bei der ersten Benutzung eines Schlosses werden das Ablaufdatum ("Gültig bis" -Datum) und der aktuelle Index des Datenträgers im Schloss gespeichert. Der Gast kann das Schloss ab dem "gültig ab" Datum nach Bedarf sperren und entsperren, so lange das Ablaufdatum nicht erreicht oder überschritten ist.

HINWEIS! Die Uhrzeit im Schloss wird ohne Berücksichtigung der Sommerzeit eingestellt! Dies ist bei der Auswertung der Buchungen sowie auch beim Berechtigen von Datenträgern mit Gültigkeitsdatum zu beachten.

Eine unbegrenzte Anzahl ⁽¹⁾ an Datenträger (Personen) können denselben Schrank benutzen. Für die Datenträger gelten in diesem Mode folgende Bedingungen:

- > Selbe Schranknummer auf den Datenträgern
- > Selbes Gültigkeitsdatum auf den Datenträgern
- > Selber Indexwert auf den Datenträgern ⁽²⁾

⁽¹⁾ Bei LEGIC prime Systemen ist die Anzahl der nutzbaren Datenträger auf 32 Stück begrenzt, da das Schloss zusätzlich die Unikatsnummer der berechtigten Datenträger speichert.

⁽²⁾ Bei LEGIC prime Systemen nicht enthalten. Die Erkennung der Datenträger erfolgt über die Schranknummer und das Gültigkeitsdatum.

Sobald am Schloss einer dieser Datenträger das erste Mal gelesen werden, wird das Gültigkeitsdatum und der Indexwert des Datenträgers im Schloss gespeichert.

HINWEIS! Bei LEGIC prime Systemen werden die Berechtigungen nach dem Einlesen in das Schloss vom Datenträger gelöscht.

Verriegeln und Entriegeln eines Schanks

- ▶ Schließen Sie die Schranktür.
- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem Datenträger ein.
 - Die Informationen auf dem Datenträger werden gelesen. Die Schranknummer auf dem Datenträger muss mit der Schranknummer des Schlosses übereinstimmen.
- ▶ Es sind folgende Situationen möglich. Der Datenträger ...
 - 1) ... ist der erste, der am Schloss gelesen wird:
 - Index und Gültigkeitsdatum des Datenträgers werden im Schloss gespeichert. Der Datenträger kann den Schrank dann bis zum Ablauf der Gültigkeitsdauer ver- und entriegeln.
 - 2) ... hat selben Index und selbes "gültig bis" Datum wie im Schloss:
 - Der Datenträger kann den Schrank gleichberechtigt mit den anderen Datenträgern ver- und entriegeln.
 - 3) ... hat höheren Index-Wert als der im Schloss gespeicherte Index:
 - Der neue Index-Wert und das "gültig bis" Datum des Datenträgers werden im Schloss gespeichert. Die zuvor am Schloss berechtigten Datenträger verlieren ihre Gültigkeit, d.h. sie haben dann keine Berechtigung mehr für das Schloss.

- 4) ... hat gleichen Index und höheres "gültig bis" Datum als das Schloss:
- o Der Index-Wert und das neue "gültig bis" Datum des Datenträgers werden im Schloss gespeichert. Die zuvor am Schloss berechtigten Datenträger verlieren ihre Gültigkeit, d.h. sie haben dann keine Berechtigung mehr für das Schloss.

HINWEIS! Die Situation 2) ist möglich, wenn der Schrank gesperrt oder offen ist. Situationen 3) und 4) sind bei offenem und versperrem Schrank möglich, mit der Ausnahme, wenn das "PersonalLockerSecureFlag" gesetzt ist (siehe "2.4.12. Konfigurationseinstellungen"). Mit gesetztem Flag ist dieser Vorgang nur bei offenem (unversperrem) Schrank möglich.

- ▶ Lassen Sie die Schranktür los.
 - a) Gültiger Datenträger: Der Schrankzustand wird gewechselt, das heißt dass der Schrank geöffnet wird, wenn er versperrt war, und versperrt wird, wenn er offen war.
 - b) Ungültiger Datenträger: Die LED leuchtet kurz rot auf und das Schloss wird ohne Durchführung einer Aktion wieder ausgeschaltet.

Es gibt keine unbegrenzte Vermietdauer, d.h. das Ablaufdatum muss ein gültiges Datum sein (nicht "0"). Wenn das "gültig bis" Datum überschritten ist kann der Schrank nicht mehr mit dem Datenträger geöffnet werden, außer das "LastOpenAtExpiredDate" Flag ist gesetzt (siehe "2.4.12. Konfigurationseinstellungen"). In diesem Fall kann der Schrank noch einmal mit dem Datenträger geöffnet werden.

HINWEIS! Der PROGRAM Datenträger kann für die Einstellung "Personal locker mode - Expiry date" verwendet werden, um den Index des Schlosses auf 0 zurückzusetzen.

HINWEIS! Der PROGRAM Datenträger löscht bei LEGIC Prime Systemen alle gespeicherten Berechtigungen aus dem Schloss.

3.7 GAT ECO.Basic Set

Das GAT ECO.Basic Set ist für alle Gantner Batterieschrankschlösser ohne CardNET-Funktion und OSS Standard Online-Funktion vorgesehen. Je nach gewünschter RFID-Technologie stehen zwei GAT ECO.Basic Sets zur Verfügung:

- > Für LEGIC advant: GAT ECO.Basic Set BA lite (Artikel-Nr. 1110090)
- > Für MIFARE DESFire: GAT ECO.Basic Set FD lite (Artikel-Nr. 1110092)

Im GAT ECO.Basic Set sind die folgenden Artikel enthalten oder können zusätzlich separat bestellt werden.

System-Datenträger enthalten in den Basic Sets:

- > MASTER Datenträger (rot, 3 Stück)
- > DELETE MASTER Datenträger (orange)
- > PROGRAM Datenträger (schwarz)
- > BATTERY Datenträger (blau)
- > SERVICE Datenträger (gelb)
- > APP KEY Datenträger (violett)

Weitere in den Basic Sets enthaltene Artikel:

- > 3 m USB-Programmierkabel
- > Gantner Schlüsselband
- > Batteriefachschlüssel metall, kein RFID, "GL7p Battery CoverKey" (Art.-Nr. 749230)
- > Batteriefachschlüssel mit RFID "GAT ECO.Lock 7000 - Battery Key GEA" (Art.-Nr. 920827)

Optionale Datenträger:

- > OPEN MASTER Datenträger
- > Batteriefachschlüssel metall, kein RFID, "GL7p Battery CoverKey" (Art.-Nr. 749230)
- > Batteriefachschlüssel metall, kein RFID, "GAT ECO.Lock 7000 Battery Key metal" (Art.-Nr. 616526)
- > Notstromadapter GAT ECO.EPS 7000, nur für GAT ECO.Lock 7xxx (Art.-Nr. 963733)
- > Notstromadapter GAT ECO.SPS 7000, nur für GAT ECO.Side Lock 7xxx (Art.-Nr. 1110727)

3.8 Informationen zu den Systemdatenträgern

Die im GAT ECO.Basic Set enthaltenen Datenträger werden benötigt, um eine Schrankanlage, die mit GANTNER-Batterieschlössern ausgestattet ist, zu konfigurieren und zu warten.

HINWEIS!

- > Die Systemdatenträger sind anlagenspezifisch codiert und funktionieren nur mit dem jeweiligen System.
- > Um die Sicherheit des Schranksystems zu gewährleisten, stellen Sie sicher, dass alle im GAT ECO.Basic Set enthaltenen Systemdatenträger an einem sicheren Ort aufbewahrt werden, der vor unbefugtem Zugriff geschützt ist.

3.8.1 MASTER Datenträger

Mit einem MASTER Datenträger können alle Schlösser einer Anlage geöffnet und gesperrt werden. Falls ein Datenträger eines Benutzers verloren geht, kann mittels eines MASTER Datenträgers eine Notöffnung durchgeführt werden. Im GAT ECO.Basic Set sind drei MASTER Datenträger enthalten, die nur in der jeweiligen Anlage gültig sind.

HINWEIS! Wenn im Schloss der Batteriealarm aktiv ist, kann das Schloss nicht mehr verspermt werden. Ein gültiger MASTER oder OPEN MASTER Datenträger aktiviert in diesem Zustand immer den Öffnungsmechanismus, auch wenn das Schloss bereits geöffnet ist.

Nach Verlust eines MASTER Datenträgers kann bei Gantner Electronic GmbH ein neuer MASTER Datenträger bestellt werden. Vor der ersten Verwendung des neuen MASTER Datenträgers an einem Schloss müssen zuerst alle "alten" MASTER Datenträger mit dem DELETE MASTER (RESET) Datenträger aus dem Schloss gelöscht und danach alle neuen (bzw. die bisherigen noch gültigen) MASTER Datenträger im Schloss gespeichert werden. Führen Sie dazu folgende Schritte aus:

- ▶ Aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem DELETE MASTER (RESET) Datenträger ein.
 - Die Informationen auf dem Datenträger werden gelesen und die LED blinkt rot, bis der DELETE MASTER (RESET) Datenträger entfernt wird.
- ▶ Entfernen Sie den DELETE MASTER (RESET) Datenträger vom Schloss.
 - Alle MASTER Datenträger wurden gelöscht. Danach fängt die LED an abwechselnd rot/grün zu blinken. Nun können die neuen MASTER Datenträger eingelernt werden.
- ▶ Innerhalb von 5 Sekunden aktivieren Sie das Schloss ca. 1 Sekunde lang mit dem ersten MASTER Datenträger ein.
 - Die LED leuchtet grün für 2 Sekunden, wenn der Datenträger korrekt erkannt.
- ▶ Nehmen Sie den MASTER Datenträger vom Schloss.
 - Die LED blinkt abwechselnd grün und rot. Der zweite MASTER Datenträger kann jetzt einprogrammiert werden.
- ▶ Wiederholen Sie diesen Vorgang bis alle MASTER (oder auch OPEN MASTER) Datenträger eingelernt wurden.
- ▶ Wenn nach dem Einlernen eines MASTER Datenträgers länger als 5 Sekunden gewartet wird, wechselt das Schloss automatisch wieder in den normalen Betriebsmodus und die neuen MASTER Datenträger werden gespeichert.

3.8.2 OPEN MASTER Datenträger (Optionales Zubehör)

Der OPEN MASTER Datenträger kann jedes Schloss entriegeln. Wenn ein Benutzer seinen persönlichen Datenträger verliert, kann eine Notöffnung seines Schrankes mit dem OPEN MASTER Datenträger erfolgen. Im Unterschied zum MASTER Datenträger kann der OPEN MASTER Datenträger den Schrank nach dem Öffnen nicht wieder versperren. Der OPEN MASTER Datenträger ist nicht im GAT ECO.Basic Set enthalten und muss separat bestellt werden. Dieser Datenträger ist nur für die zugeordnete Anlage gültig.

Ein OPEN MASTER Datenträger kann anstelle eines MASTER Datenträgers verwendet werden. Um einen OPEN MASTER Datenträger in ein Schloss zu programmieren, muss dieser am Schloss gelesen werden. Ist bereits die max. Anzahl MASTER Datenträger (10) programmiert, müssen zuerst alle MASTER Datenträger gelöscht und der OPEN MASTER Datenträger zusammen mit den gewünschten MASTER Datenträgern einprogrammiert werden (gesamte Anzahl = 10).

3.8.3 DELETE MASTER Datenträger

Mit dem DELETE MASTER Datenträger werden alle Masterdatenträger, die in einem Schloss gespeichert sind, gelöscht. Siehe Abschnitt "3.8.1. MASTER Datenträger".

3.8.4 PROGRAM Datenträger

Mit dem PROGRAM Datenträger können Schlösser im Modus "Persönliche Schränke" (Personal Locker) neu programmiert bzw. die bestehende Programmierung gelöscht werden. Außerdem kann er bei der Einstellung "Persönliche Schränke mit Ablaufdatum Modus" (Personal Locker Expiry Date) verwendet werden, um den Index des Schlosses auf 0 zurückzusetzen. Siehe Abschnitt "3.6.4. Personal Locker Programming Card Modus".

3.8.5 BATTERY Datenträger

Nach einem Batteriewechsel befindet sich das Schloss im Batteriewechselmode und muss mittels eines BATTERY Datenträgers wieder in den normalen Betriebsmode gesetzt werden. Der interne Betätigungszähler wird dabei auf Null gesetzt. Anweisungen dazu finden Sie im Installationshandbuch des jeweiligen Schlosses.

HINWEIS! Durch einen Batteriewechsel an einem Schloss im Modus "Persönliche Schränke" (Personal Locker) gehen die im Schloss gespeicherten Berechtigungen nicht verloren.

3.8.6 SERVICE Datenträger

Der SERVICE Datenträger wird verwendet, um das Schloss in den Konfigurationsmodus zu setzen, nachdem es an einem Computer via USB angeschlossen wurde. Anweisungen dazu finden Sie im Installationshandbuch des jeweiligen Schlosses. Die Einstellungen des Schlosses werden mit GAT ECO Lock Configurator konfiguriert, während das Schloss im Konfigurationsmodus ist (siehe "2. KONFIGURATION").

HINWEIS! Der SERVICE Datenträger muss für Servicetechniker, die das Schranksystem konfigurieren zur Verfügung stehen. Ohne den SERVICE Datenträger ist keine Systemkonfiguration möglich!

3.8.7 APP KEY Datenträger

Der APP KEY Datenträger wird für die Konfiguration eines Schlosses mit der MoLA App benötigt. Diese App kann auf einem Mobilgerät mit Android Betriebssystem installiert werden. Wenn das Schloss im Werksmodus ist und das erste Mal konfiguriert wird, wird der APP KEY nicht benötigt. Jedoch für spätere Konfigurationsänderungen benötigen Sie den APP KEY Datenträger (siehe auch "2.3. Konfiguration mit der MoLA App").



Um ein Schloss mit dem GAT ECO Lock Configurator zu konfigurieren, wird der APP KEY Datenträger nicht benötigt.

3.8.8 BLOCKING Datenträger (optionales Zubehör)

Mit diesem Datenträger kann ein Schrank, der durch einen Benutzer versperrt ist, blockiert werden. Nachdem der BLOCKING Datenträger an einem Schloss gelesen wird, kann der Benutzer seinen Schrank nicht mehr öffnen. Zum Öffnen muss ein MASTER oder OPEN MASTER Datenträger verwendet werden. Nach dem Lesen des BLOCKING Datenträgers wird auch die automatische Öffnungsfunktion solange deaktiviert, bis der Schrank mit einem MASTER oder OPEN MASTER Datenträger wieder geöffnet wird.

Der BLOCKING Datenträger ist nicht im Lieferumfang enthalten und kann als Zubehör bestellt werden.

3.9 Übersicht der Signalisierung

Jedes Schloss verfügt über eine LED und einen integrierten Piepser, die zur Anzeige der folgenden Informationen verwendet werden. Signale, die für eine Schlossvariante spezifisch sind, werden am Ende der Tabelle aufgeführt.















LED	Signalisierung	Erklärungen
	<ul style="list-style-type: none"> LED blinkt kurz blau 	Schloss aktiviert, bereit um einen Datenträger zu lesen
	<ul style="list-style-type: none"> LED leuchtet dauerhaft blau 	<ul style="list-style-type: none"> Schloss wurde mittels USB-Kabel aktiviert, jedoch ist keine USB-Kommunikation möglich Der Status bleibt ca. 1½ Minuten aktiv USB-Kabel prüfen, USB Schnittstelle am PC überprüfen
	<ul style="list-style-type: none"> LED blinkt einmal rot absteigender Signalton 	<ul style="list-style-type: none"> keine Berechtigung kein Datenträger gelesen Fehler
	<ul style="list-style-type: none"> LED blinkt einmal grün aufsteigender Signalton 	<ul style="list-style-type: none"> Datenträger akzeptiert Vorgang erfolgreich
	<ul style="list-style-type: none"> LED blinkt einmal lange grün aufsteigende Tonfolge 	<ul style="list-style-type: none"> Batteriewechsel erfolgreich mit dem BATTERY Datenträger bestätigt Batteriewarnung zurückgesetzt
	<ul style="list-style-type: none"> LED blinkt schnell rot / grün 	Schloss wartet auf einen Datenträger zum Einlernen oder Freigeben (SERVICE, MASTER, Benutzerdatenträger, ...)
	<ul style="list-style-type: none"> LED blinkt 4 x rot 5 Signaltöne 	Batteriewechsel notwendig
	<ul style="list-style-type: none"> LED blinkt mehrfach hintereinander kurz grün 	<ul style="list-style-type: none"> Verriegelung per App aktiviert Schloss verschließt automatisch, wenn es betätigt wird
	<ul style="list-style-type: none"> LED blinkt grün, abwechselnd zwischen hell und dunkel 	USB Kommunikationsmode aktiv
	<ul style="list-style-type: none"> LED blinkt schnell rot 	<ul style="list-style-type: none"> Bootloader aktiv Firmware kann geladen werden
	<ul style="list-style-type: none"> LED blinkt schnell hell/dunkel rot 	<ul style="list-style-type: none"> Firmware wird geladen Kommunikation zum Schloss aktiv
GL7p		
	<ul style="list-style-type: none"> LED blinkt kurz weiß kurzer Signalton 	Druck einer PIN-Code Taste wurde erkannt
GAT ECO.Side Lock		
	<ul style="list-style-type: none"> LED blinkt einmal orange 	Schloss ist bereit für einen Datenträger
	<ul style="list-style-type: none"> LED blinkt dauernd rot Dauerndes hoch / tief Tonintervall 	<ul style="list-style-type: none"> Einbruchsalarm ausgelöst Alarm mittels gültigen MASTER Datenträger quittieren

Tabelle 3.2 – Übersicht der Signalisierung



**GLOBALES
PARTNERNETZWERK**



**40+
NIEDERLASSUNGEN**



**40.000+
PROJEKTE WELTWEIT**



**40+ MILLIONEN
NUTZER TÄGLICH**

SCAN FOR CONTACT



gantner 

INSPIRED ACCESS

www.gantner.com

©2026 Gantner®

Gantner reserves the right to change technical specifications, designs and services without prior notice.

Photos: Gantner, Salto Systems, Shutterstock

SALTO WECOSYSTEM