

100 Gesichts-erkennungen

200 Fingerab-drücke

1000 NFC Karten

200 Zugangs-code

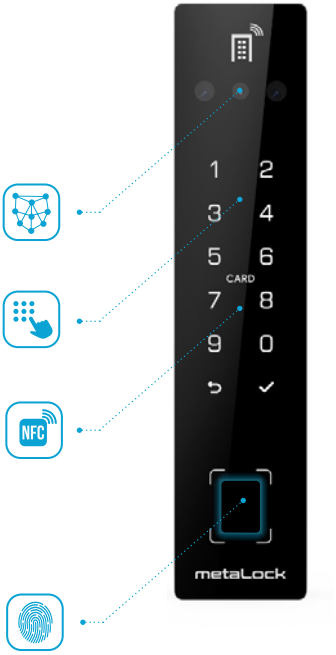
HANDBUCH

metaLock®

SMART READER 2.0

TTLOCK APP

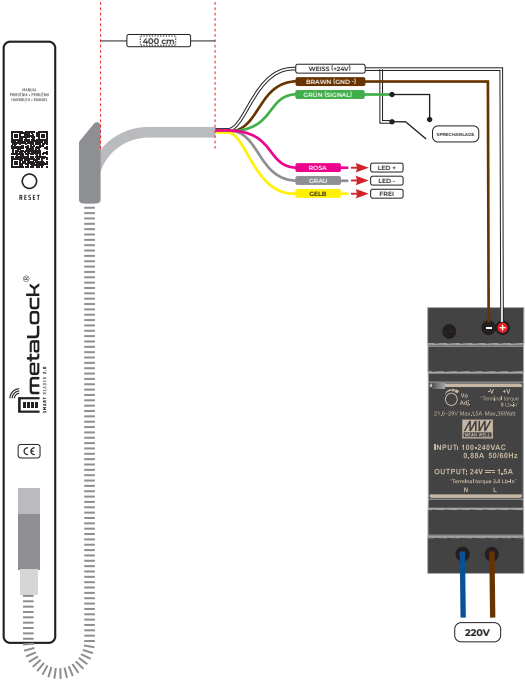
Zum Herunterladen der App scannen



Handbuch

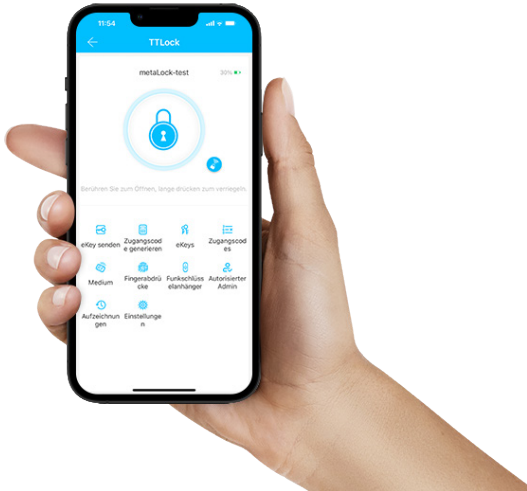
metaLock®

SCHALTPLAN



EINLEITUNG

Die App ist eine intelligente Schlossverwaltungs-software, die von Shenzhen Smarter Intelligent Control Technology Co., Ltd. entwickelt wurde. Sie umfasst Türschlösser, Parkschlösser, Tresorschlösser, Fahrradschlösser und mehr. Die App kommuniziert mit dem Schloss über Bluetooth BLE und kann entsperren, sperren, Firmware aktualisieren, Betriebsaufzeichnungen lesen usw. Der Bluetooth-Schlüssel kann auch das Türschloss über die Uhr öffnen. Die Anwendung ist mehrsprachig.



INHALT

REGISTRIERUNG, AUTHENTIFIZIERUNG UND ANMELDEN 6

LUCIN ERFOLGREICH 7

SCHLOSSVERWALTUNG 8

HINZUFÜGEN SPERREN 9

AKTUALISIERUNG DER SPERRE UND ZEITKALIBRIERUNG 11

AUTORISIERTER ADMINISTRATOR 12

SCHLÜSSELVERWALTUNG 13

PASSCODE-MANAGER 14

KARTENVERWALTUNG 17

VERWALTUNG: GESICHTSERKENNUNG / FINGERABDRUCK 17

ÜBER BLUETOOTH FREISCHALTEN 18

SYSTEMEINSTELLUNGEN 18

PASSAGE-MODUS 19

ANWESENHEITSMANAGEMENT 19

ADMIN-RECHTE ÜBERTRAGEN 20

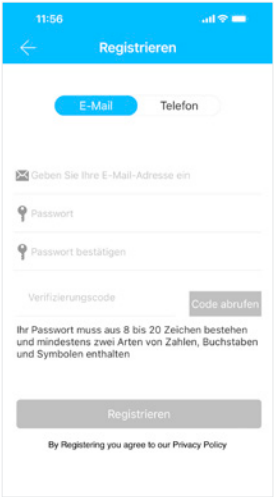
GATEWAY-VERWALTUNG 20

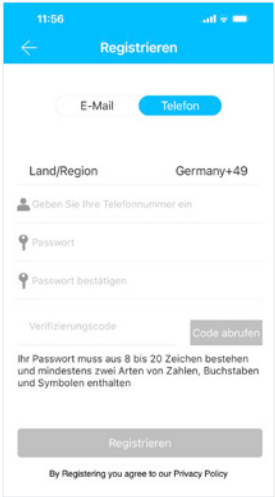
LICHTSTATUS 21

KOPPELN SIE DAS GATEWAY MIT DER APP 21

REGISTRIERUNG, AUTHENTIFIZIERUNG UND ANMELDEN

Benutzer können das Konto per Mobiltelefon und E-Mail registrieren, das derzeit 200 Länder und Regionen der Welt unterstützt. Der Verifizierungscode wird an das Mobiltelefon oder die E-Mail des Benutzers gesendet und die Registrierung ist nach der Verifizierung erfolgreich.

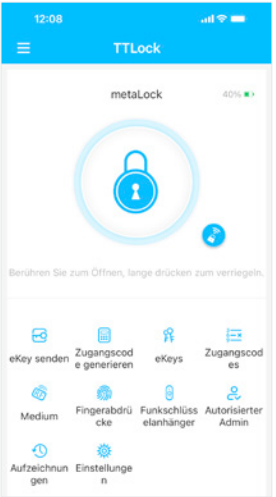




LUCIN ERFOLGREICH

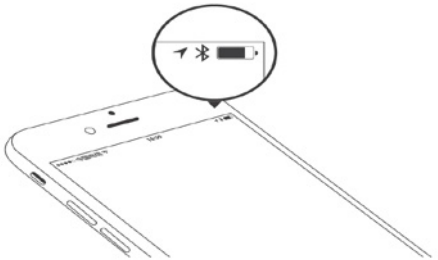
Wenn Sie die Schlossschloss-App zum ersten Mal verwenden und keine Schloss- oder Schlüsseldaten im Konto vorhanden sind, wird auf der Startseite die Schaltfläche zum Hinzufügen des Schlosses angezeigt. Wenn das Konto bereits ein Schloss oder einen Schlüssel enthält, werden die Schlossinformationen angezeigt.





SCHLOSSVERWALTUNG

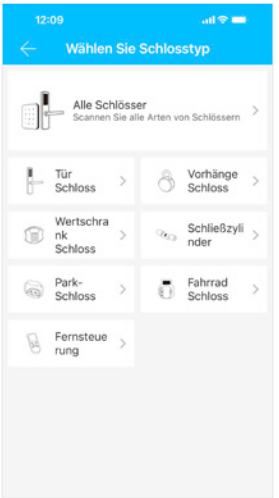
Die Sperre muss in der App hinzugefügt werden, bevor sie verwendet werden kann. Das Hinzufügen eines Schlosses bezieht sich auf die Initialisierung des Schlosses durch die Kommunikation mit dem Schloss über Bluetooth. Bitte stellen Sie sich neben das Schloss. Sobald das Schloss erfolgreich hinzugefügt wurde, können Sie das Schloss mit der App verwalten, einschließlich des Sendens eines Schlüssels, des Sendens eines Passworts usw.



Wenn das Schloss hinzugefügt wird, wird der Addierer zum Administrator des Schlosses. Gleichzeitig kann das Schloss nicht durch Berühren der Tastatur in den Setup-Modus wechseln. Diese Sperre kann erst wieder hinzugefügt werden, nachdem der aktuelle Administrator die Sperre gelöscht hat. Das Löschen des Schlosses muss über Bluetooth neben dem Schloss erfolgen.

HINZUFÜGEN SPERREN

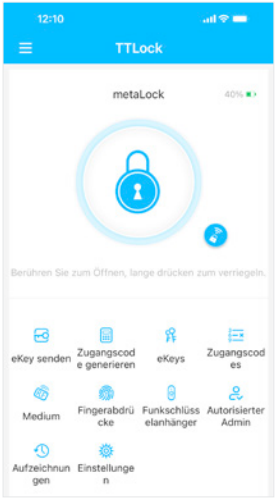
Die App unterstützt mehrere Arten von Schlössern, darunter Türschlösser, Vorhängeschlösser, Tresorschlösser, intelligente Schließzylinder, Parkschlösser und Fahrradschlösser. Beim Hinzufügen eines Geräts müssen Sie zunächst den Sperrtyp auswählen. Das Schloss muss nach dem Aufrufen des Einstellungsmodus zur App hinzugefügt werden. Eine nicht hinzugefügte Sperre wechselt in den Einstellungsmodus, solange die Sperrtastatur berührt wird.





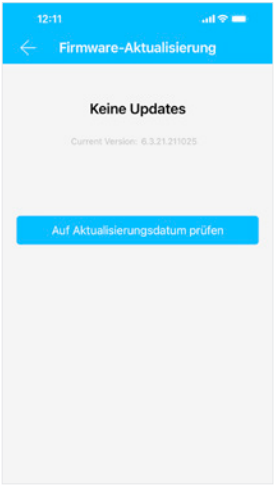
Weisen Sie Ihrem Schloss einen Namen zu und Sie sehen einen Hauptbildschirm.

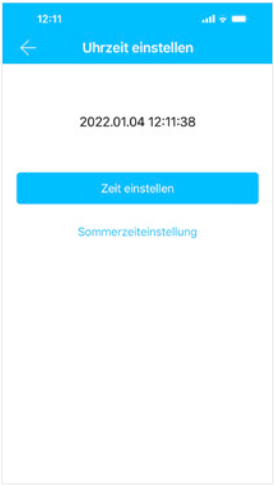




AKTUALISIERUNG DER SPERRE UND ZEITKALIBRIERUNG

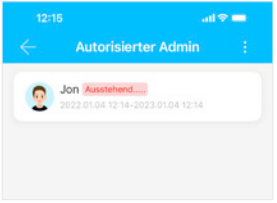
Der Benutzer kann die Schlosshardware in der APP aktualisieren. Das Upgrade muss über Bluetooth neben dem sperren. Wenn das Upgrade erfolgreich ist, können der ursprüngliche Schlüssel, das Kennwort, die IC-Karte und der Fingerabdruck weiter verwendet werden. Wenn ein Gateway vorhanden ist, wird die Uhr zuerst über das Gateway kalibriert. Wenn kein Gateway vorhanden ist, muss es über das Bluetooth des Mobiltelefons kalibriert werden.

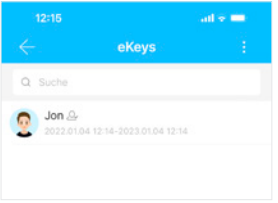




AUTORISIERTER ADMINISTRATOR

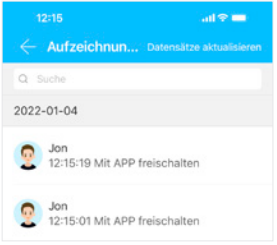
Nur der Administrator kann den Schlüssel autorisieren. Bei erfolgreicher Autorisierung stimmt der autorisierte Schlüssel mit der Benutzeroberfläche des Administrators überein. Er kann Schlüssel an andere senden, Passwörter senden und vieles mehr. Der autorisierte Administrator kann jedoch andere nicht mehr autorisieren.





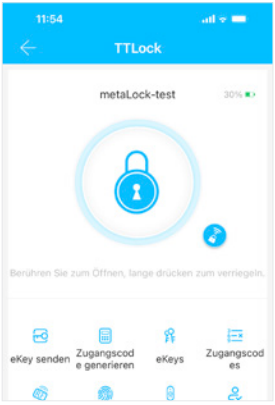
SUCHSPERRE AUFZEICHNUNG

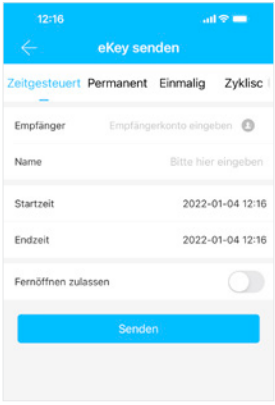
Der Administrator kann den Entsperrdatensatz jedes Schlüssels abfragen.



SCHLÜSSELVERWALTUNG

Nachdem der Administrator die Sperre erfolgreich hinzugefügt hat, besitzt er die höchsten Administratorrechte für die Sperre. Er kann anderen Schlüssel schicken. In der Zwischenzeit kann er die auslaufende Schlüsselverwaltung erhöhen. Klicken Sie

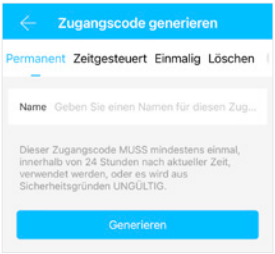




auf die Art des Schlosses, es wird der zeitlich begrenzte ekey angezeigt, einmaliger ekey und permanenter ekey. **Zeitlich begrenzter ekey**: Der ekey ist für die angegebene Zeit gültig, **Dauerhafter ekey**: Der ekey kann dauerhaft verwendet werden. **Einmaliger ekey**: Der ekey wird nach Gebrauch automatisch gelöscht. **Wiederkehrender ekey**: Der Schlüssel arbeitet an bestimmten Tagen und Uhrzeiten.

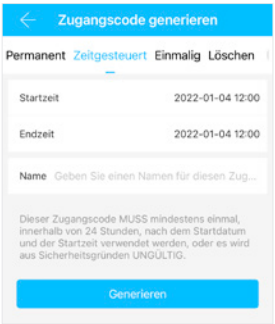
PASSCODE-MANAGER

Drücken Sie nach der Eingabe des Passcodes auf der Tastatur des Schlosses die Entriegelungstaste, um es zu entriegeln. Passcodes werden in permanente, zeitlich begrenzte, einmalige, löschbare, benutzerdefinierte usw.



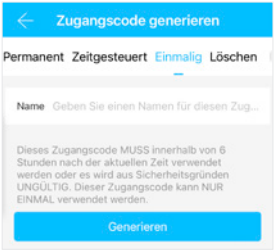
Permanenter Passcode

Der permanente Passcode muss innerhalb von 24 Stunden nach der Generierung verwendet werden, andernfalls verfällt er automatisch.



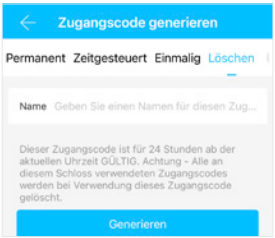
Zeitlich begrenzter Passcode

Der zeitlich begrenzte Passcode kann ein Ablaufdatum besitzen, das mindestens eine Stunde und höchstens drei Jahre beträgt. Liegt die Gültigkeitsdauer innerhalb eines Jahres, die Zeit kann auf die Stunde genau sein; beträgt die Gültigkeitsdauer mehr als ein Jahr, beträgt die Genauigkeit einen Monat. Wenn der zeitlich begrenzte Passcode gültig ist, sollte er lauten innerhalb von 24 Stunden verbraucht, sonst es verfällt automatisch.



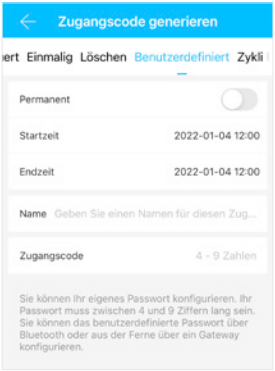
Einmaliger Passcode

Der einmalige Passcode kann nur einmal verwendet werden und ist 6 Stunden lang verfügbar.



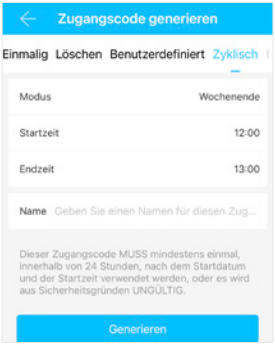
Passcode löschen

Passcode löschen wird verwendet, um alle Passcodes zu löschen, die von der Sperre festgelegt wurden und die 24 Stunden lang verfügbar sind.



Benutzerdefinierter Passcode

Der Benutzer kann beliebige Passcodes festlegen und Gültigkeitsdauer er will.

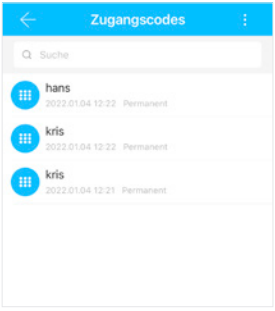


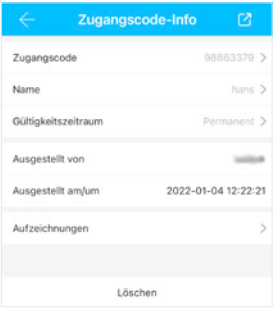
Wiederkehrender Passcode

Der wiederkehrende Passcode kann innerhalb einer bestimmten Zeitraum, einschließlich täglich Typ, Wochentagtyp, Wochenendtyp und mehr.

PASSCODE-MANAGER

Alle generierten Passwörter können im Passwortverwaltungsmodul eingesehen und verwaltet werden. Dies beinhaltet das Recht, das Passwort zu ändern, das Passwort zu löschen, das Passwort zurückzusetzen und das Passwort zu entsperren.

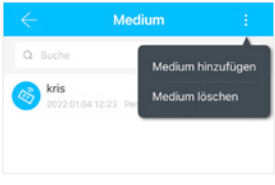




KARTENVERWALTUNG

Sie müssen zuerst die NFC-Karte hinzufügen. Der gesamte Vorgang muss über die App neben dem Schloss durchgeführt werden. Die Gültigkeitsdauer der NFC-Karte kann entweder dauerhaft, zeitlich begrenzt oder wiederkehrend eingestellt werden.

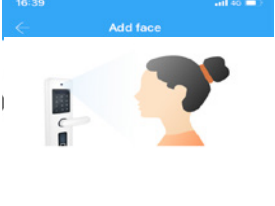


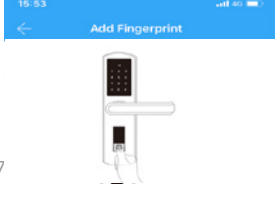


Alle NFC-Karten können über das Kartenverwaltungsmodul abgefragt und verwaltet werden.

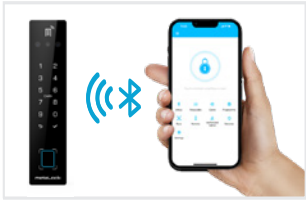
VERWALTUNG: GESICHTSERKENNUNG / FINGERABDRUCK

Die Verwaltung per Gesichtserkennung oder Fingerabdruck funktioniert ähnlich wie die Verwaltung der NFC-Karten. Nach dem Hinzufügen eines Gesichtsbildes oder Fingerabdrucks kann damit die Tür geöffnet werden.





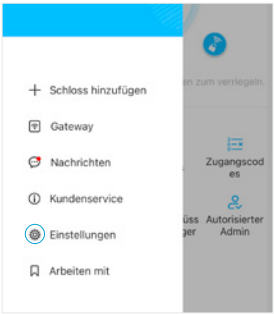
ÜBER BLUETOOTH FREISCHALTEN



App-Nutzer können die Tür über Bluetooth entriegeln und den Bluetooth ekey auch an jeden senden. Klicken Sie auf den runden Knopf oben auf der Seite, um die Tür zu entriegeln, und halten Sie den runden Knopf gedrückt, um die Tür zu verriegeln. Da das Bluetooth-Signal eine gewisse Reichweite hat, verwenden Sie bitte die APP innerhalb des bestimmten Bereichs.

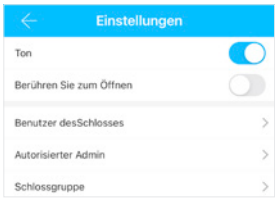
SYSTEMEINSTELLUNGEN

In den Systemeinstellungen umfasst es Touch-Entsperrschalter, Gruppenverwaltung, Gateway-Verwaltung, Sicherheitseinstellungen, Erinnerung, Smart Lock übertragen und so weiter.



Touch to unlock

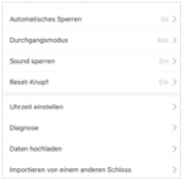
Touch unlock setting determines whether you can open the door by touching the lock.

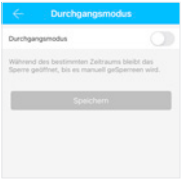


PASSAGE-MODUS

Während des bestimmten Zeitraums bleibt das Schloss entsperrt, bis es manuell gesperrt wird.

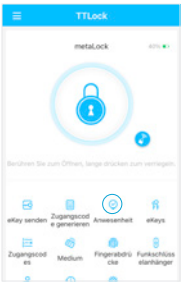


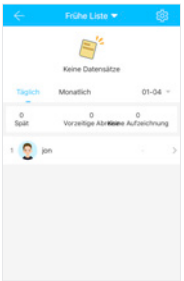




ANWESENHEITSMANAGEMENT

Die APP ist eine Zugangskontrolle, die für das Anwesenheitsmanagement des Unternehmens verwendet werden kann. Die App enthält Funktionen zur Personalverwaltung, Anwesenheitsstatistik und so weiter. Der normale Türschlossbesuch Funktion ist standardmäßig deaktiviert. Der Benutzer kann es in den Sperreinstellungen ein- oder ausschalten.

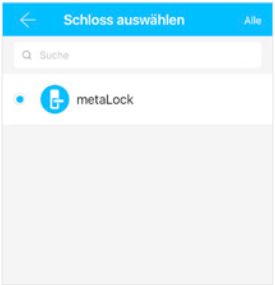


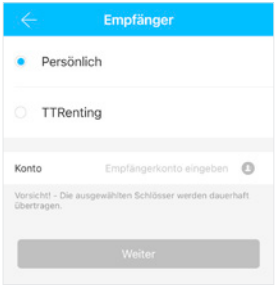




ADMIN-RECHTE ÜBERTRAGEN

Der Administrator kann die Sperre auf andere Benutzer übertragen. Nur das Konto, das die Sperre verwaltet, hat das Recht, die Sperre zu übertragen.





GATEWAY-VERWALTUNG

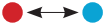


Das Smart Lock ist direkt über Bluetooth verbunden, weshalb es vom Netzwerk nicht angegriffen wird. Das Gateway ist eine Brücke zwischen Smart Locks und Heim-WIFI-Netzwerken. Über das Gateway kann der Benutzer die Sperruhr aus der Ferne anzeigen und kalibrieren sowie den Entsperrdatensatz lesen. Inzwischen, es kann das Kennwort aus der Ferne löschen und ändern.

LICHTSTATUS

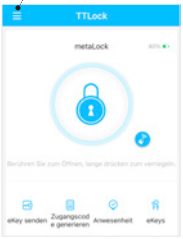


Wenn das Gateway eingeschaltet ist:

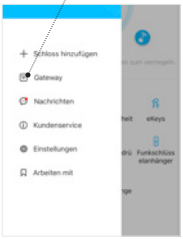
	Licht blinkt abwechselnd rot und blau: Stand-by-Modus, Pairing-Modus
	Blaues Licht: Arbeitsmodus
	Rotes Licht: Netzwerkfehler

KOPPELN SIE DAS GATEWAY MIT DER APP

Drücken



Drücken



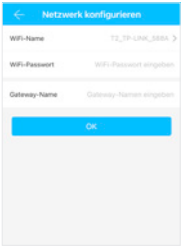
Wählen (G2)



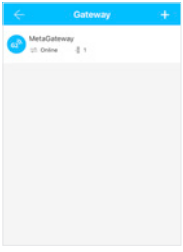
An Strom anschließen



Mit WLAN verbinden



Vollendet



FCC-ERKLÄRUNG

Dieses Gerät entspricht Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen und (2) dieses Gerät muss alle empfangenen Störungen akzeptieren, einschließlich Störungen, die einen unerwünschten Betrieb verursachen können. Änderungen oder Modifikationen an diesem Gerät, die nicht ausdrücklich von der für die Konformität verantwortlichen Partei genehmigt wurden, können die Berechtigung des Benutzers zum Betrieb des Geräts erlöschen lassen.

HINWEIS: Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte sollen einen angemessenen Schutz gegen schädliche Interferenzen bei einer Installation in Wohngebieten bieten. Dieses Gerät erzeugt, verwendet und kann Hochfrequenzenergie abstrahlen und kann, wenn es nicht gemäß den Anweisungen installiert und verwendet wird, schädliche Interferenzen bei der Funkkommunikation verursachen. Es gibt jedoch keine Garantie dafür, dass bei einer bestimmten Installation keine Interferenzen auftreten. Wenn dieses Gerät schädliche Interferenzen beim Radio- oder Fernsehempfang verursacht, die durch Aus- und Einschalten des Geräts festgestellt werden können, wird dem Benutzer empfohlen, zu versuchen, die Interferenzen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus oder verlegen Sie sie.
- Vergrößern Sie den Abstand zwischen Gerät und Empfänger.
- Schließen Sie das Gerät an eine Steckdose eines anderen Stromkreises als der des Empfängers an.
- Wenden Sie sich an den Händler oder einen erfahrenen Radio-/TV-Techniker, um Hilfe zu erhalten.

Dieses Gerät und seine Antenne(n) dürfen nicht zusammen mit anderen Antennen oder Sendern aufgestellt oder betrieben werden. Dieses Gerät entspricht Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Interferenzen verursachen und (2) dieses Gerät muss alle empfangenen Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können für eine unkontrollierte Umgebung. Dieses Gerät sollte mit einem Mindestabstand von 20 cm zwischen dem Strahler und Ihrem Körper installiert und betrieben werden.



metaLock

delutech®

DELUTECH d.o.o. • Pod jelšami 2 • SI - 1218 Komenda
+386 (0) 64 164 123 • info@delutech.si • www.delutech.si