Zamek kodowy
YD100

UWAGI WSTĘPNE

Przed montażem, podłączeniem i użytkowaniem urządzenia prosimy o dokładne zapoznanie się z niniejszą instrukcją obsługi. W razie jakichkolwiek problemów ze zrozumieniem jej treści prosimy o skontaktowanie się ze sprzedawcą urządzenia.

Samodzielny montaż i uruchomienie urządzenia jest możliwe pod warunkiem używania odpowiednich narzędzi. Niemniej zalecane jest dokonywanie montażu urządzenia przez wykwalifikowany personel.

Producent nie odpowiada za uszkodzenia mogące wyniknąć z nieprawidłowego montażu, czy eksploatacji urządzenia oraz z dokonywania samodzielnych napraw i modyfikacji.

1. OGÓLNA CHARAKTERYSTYKA I PRZEZNACZENIE

Zamek szyfrowy wraz z towarzyszącą mu aplikacją mobilną TTLock przeznaczony jest do realizacji funkcji fizycznej kontroli dostępu.

Może pracować samodzielnie, a także jako część bardziej rozbudowanego systemu. Kontrola dostępu może być realizowana zdalnie za pomocą smartfona lub fizycznie za pomocą breloka zbliżeniowego (pracującego w standardzie Mifare 13,56 MHz) lub kodu cyfrowego PIN.

Wszystkie funkcje urządzenia programuje się przy użyciu aplikacji mobilnej TTLock dostępnej na platformy iOS i Android, która komunikuje się z zamkiem za pomocą standardu Bluetooth. Aplikacja umożliwia nadawanie uprawnień innym użytkownikom, generowanie kodów PIN i przesyłaniem ich m.in. za pomocą wiadomości SMS.

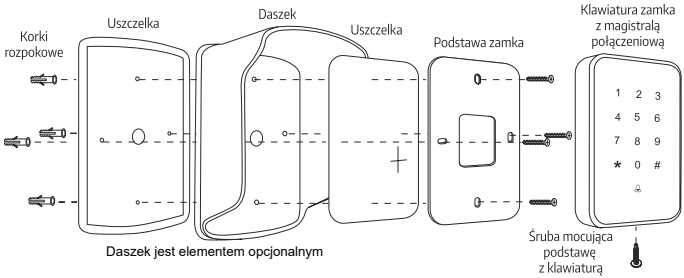
Oprócz podstawowych funkcji kontroli dostępu zamek szyfrowy wyposażony jest w funkcję rejestracji czasu pracy (RCP) umożliwiającą wgląd w historię wejść i wyjść osób objętych wymogiem weryfikacji czasu spędzonego w strzeżonym obiekcie.

Urządzenie posiada funkcję dzwonka oraz jedno wyjście przekaźnikowe, które może sterować jedną strefą (np. ryglem elektromagnetycznym przy furtce, automatem bramy, czy uzbrajaniem i rozbrajaniem centrali alarmowej itp.).

2. BUDOWA I INSTALACJA

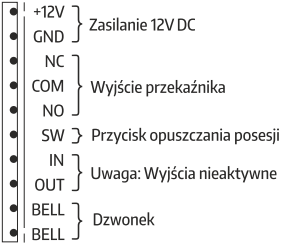
2.2. INSTALACJA

2.2.1. Przykleić szablon i nawiercić otwory o średnicy 5 mm,
2.2.2. odkręcić śrubę łączącą podstawę mocującą zamka z jego głównym korpusem znajdującą się u dołu urządzenia,
2.2.3. wprowadzić kołki rozporowe we wcześniej przygotowane otwory i przykręcić uszczelkę, daszek i podstawę zamka – Rys. 2,
2.2.4. przez otwór znajdujący się na środku podstawy przeprowadzić wszystkie niezbędne przewody połączeniowe - Rys. 2,
2.2.5. za pomocą wkrętów (wyposażenie zestawu) przymocować podstawę zamka do ściany,
2.2.6. zgodnie z wybranym schematem połączeniowym podłączyć poszczególne przewody do zacisków urządzenia,
2.2.7. umieścić główny korpus zamka z klawiaturą sensoryczną na podstawie mocującej i przykręcić śrubę mocującą u dołu zamka.



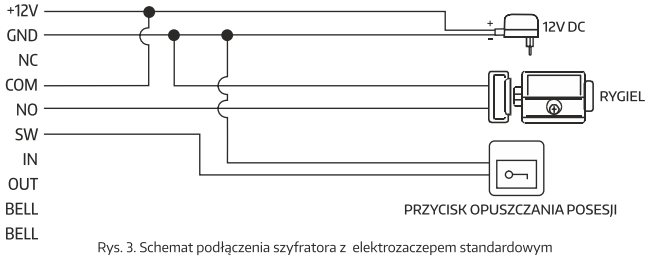
Rys.2.

OPIS STYKÓW SZYFRATORA

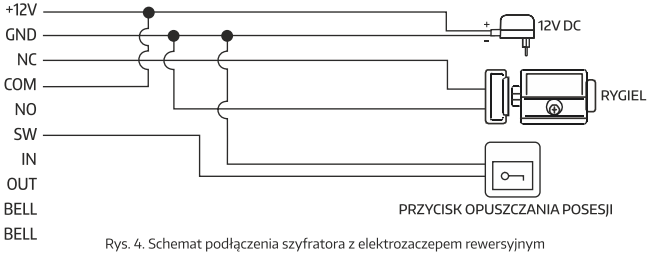


UWAGA
Wszystkie niewykorzystane żyły przewodu kostki połączeniowej należy odpowiednio zaizolować.

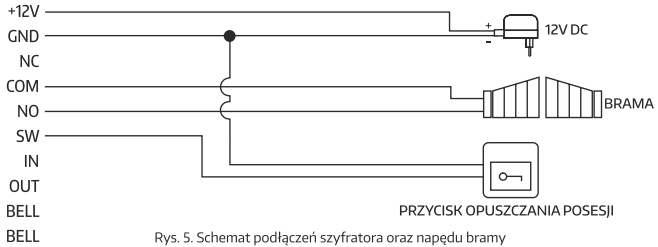
2.3. SCHEMAT PODŁĄCZENIOWY ZACISKÓW ELEKTRYCZNYCH



Rys. 3. Schemat podłączenia szyfratora z elektrozaczepem standardowym



Rys. 4. Schemat podłączenia szyfratora z elektrozaczepem rewersyjnym



Rys. 5. Schemat podłączeń szyfratora oraz napędu bramy

3. PROGRAMOWANIE I OBSŁUGA

W celu zaprogramowania urządzenia należy pobrać aplikację TTLock z GooglePlay lub z AppStore, a następnie postępować zgodnie z poniższą instrukcją.

3.1. REJESTRACJA KONTA W APLIKACJI MOBILNEJ TTLOCK

3.1.1. W prawym górnym rogu aplikacji należy kliknąć „Register",
3.1.2. należy wybrać sposób rejestracji telefoniczny/ e-mailowy,
3.1.3. wpisać numer telefonu /adres e-mail,
3.1.4. ustanowić hasło,
3.1.5. pobrać kod weryfikacyjny klikając „Get code",
3.1.6. wprowadzić kod otrzymany SMS'em /e-mailem,
3.1.7. wpisać odpowiedzi na pytania pomocnicze w przypadku zagubienia hasła – odpowiedzieć na 3 pytania wybrane z listy podpowiedzi.

3.2. LOGOWANIE DO APLIKACJI TTLOCK

Po założeniu konta należy zalogować się do aplikacji wpisując login, tj. nr telefonu / adres e-mail oraz ustanowione hasło.

3.3. DODAWANIE URZĄDZENIA DO APLIKACJI TTLOCK

Pierwsze dodawanie:

W przypadku dodawania pierwszego urządzenia na głównym ekranie aplikacji należy kliknąć w dużą ikonkę z napisem „+Add lock", a następnie należy przejść do ptk. 3.3.3

Dodawanie kolejnych urządzeń:

3.3.1. W lewym górnym rogu aplikacji należy kliknąć ikonkę z „użytkownikiem", po czym pojawi się główne menu aplikacji.
3.3.2. Z głównego menu należy wybrać pierwszą pozycję „+ Add locks".
3.3.3. Jeżeli Bluetooth nie jest włączony, aplikacja zapyta o włączenie, aby dodać zamek należy wyrazić zgodę.
3.3.4. Z listy urządzeń należy wybrać pierwszą pozycję „Door Lock".
3.3.5. Teraz należy dotknąć klawiatury dodawanego urządzenia (tj. szyldu) w celu wprowadzenia elektroniki w stan parowania.
3.3.6. Po zakończeniu wyszukiwania, aplikacja wyświetli listę znalezionych urządzeń.
3.3.7. Z listy należy wybrać dodawane urządzenie. Uwaga: W celu bezproblemowego przejścia przez proces parowania urządzenia należy dodawać pojedynczo.
3.3.8. Po wyborze urządzenia aplikacja automatycznie przeniesie nas do głównego menu.

3.4 OPCJE UŻYTKOWNIKA

Bezpośrednio po otwarciu aplikacji, w jej głównym ekranie, klikając w ikonkę trzech poziomych kresek znajdujących się w lewym górnym rogu otwieramy menu użytkownika, które umożliwia:

3.4.1 „**Add lock+**" - Dodanie kolejnego urządzenia do aplikacji (z listy dostępnych urządzeń wybieramy opcję „Door Lock")

3.4.2. **Messages** – wgląd w informacje systemowe dotyczące np. migracji urządzenia na konto innego użytkownika, logowania na twoim koncie z innego urządzenia itp.

3.4.3. **Customer Service** – W tym miejscu znajdziemy FAQ, czyli odpowiedzi na najczęściej zadawane pytania

3.4.4. **Settings**:

> **Uwaga:** Wszystkie aktywowane funkcje w opcjach użytkownika są automatycznie zastosowane do wszystkich urządzeń sparowanych z aplikacją.

3.4.4.1. **Sound** – Włączanie/ wyłączanie powiadomień dźwiękowych w aplikacji,

3.4.4.2. **Touch to unlock** – funkcja umożliwiająca zwolnienie rygla po przyciśnięciu dowolnego klawisza klawiatury na ok. 3 s,
Uwaga: Opcja wymaga komunikacji aplikacji z urządzeniem, w związku z czym działa wyłącznie w przypadku gdy aplikacja TTLock jest wyłączna,

3.4.4.3. **Lock Users** – opcja wyświetla uprawnienia i umożliwia usunięcie użytkowników zamka (konta, do których został przypisany eKey),

3.4.4.4. **Lock Group** – opcja umożliwia utworzenie grup zamków np. zamki na 1 piętrze itp,

3.4.4.5. **Gateway** – opcja umożliwiająca dodanie bramki WiFi m.in. służącej do zdalnego usuwania kodów (bramka utrzymuje komunikację między urządzeniem, a aplikacją, dzięki czemu wszystkie komendy realizowane są w czasie rzeczywistym, a nie wyłącznie po synchronizacji poprzez Bluetooth),

3.4.4.6. **Transfer lock** – opcja umożliwia migrację urządzenia na konto innego użytkownika, równoznaczna jest z przekazaniem uprawnień administratora lub room mastera, aby tego dokonać należy:

3.4.4.6.1 Należy wybrać urządzenie do transferu i przejść do następnej części klikając „**Next**"

3.4.4.6.2 Wybrać rodzaj transferu: Personal (przekazanie całkowite wszystkich uprawnień administratora) lub **Room Master** (częściowe przekazanie uprawnień).

3.5. OBSŁUGA URZĄDZENIA

3.5.1. **Ikona dużej kłódki** widniejąca w górnej części ekranu aplikacji pozwala na zwolnienie zamka będącego w zasięgu nadajnika Bluetooth urządzenia na którym zainstalowana jest aplikacja.

3.5.2. **"Send eKey"** - eKey to klucze dostępu, które przesyłamy innym użytkownikom aplikacji, najczęściej dedykowane są do personelu obsługującego zabezpieczone pomieszczenie. Klucze umożliwiają otwieranie zamka będącego w zasięgu nadajnika Bluetooth, aby wysłać eKey należy:

3.5.2.1. Wybrać ikonę eKey

3.5.2.2. Wybrać rodzaj klucza, klikając pozycję „Type" - do wyboru mamy klucze:
- czasowe (timed),
- stałe (permanent),
- jednorazowe (one-time).

3.5.2.3. W polu „Account" Wpisać nazwę konta użytkownika, któremu przekazujemy klucz.

3.5.2.4. W polu „Name" należy wpisać nazwę klucza.

3.5.2.5. W przypadku wyboru klucza czasowego należy określić jego datę ważności

3.5.2.6. Wysłać klucz, klikając „Send".
W celu otwarcia drzwi korzystając z aplikacji mobilnej za pomocą eKey należy kliknąć w aplikacji mobilnej w ikonkę dużej kłódki.

3.5.3. „**Generate Passcode**" - to kody dostępu wysyłane użytkownikom szyldu (gościom, pracownikom), aby wysłać kod dostępu należy wybrać ikonę „Send Passcode", a następnie:

3.5.3.1. Wybrać rodzaj kodu:

- **permanent** – kod bezterminowy - kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność,
- **timed** – kod czasowy, kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność,
- **one-time** – kod jednorazowy – musi być użyty w przeciągu 6 godzin od ustanowienia, w przeciwanym razie traci ważność,
- **erase** – kod czyszczący – należy go użyć przed upływem 24h, w innym przypadku wygaśnie. Po jego użyciu wszystkie kody przypisane do danego urządzenia zostaną usunięte. Aby lista kodów w aplikacji została wyczyszczona należy dokonać synchronizacji aplikacji i szyldu, najłatwiej tego dokonać za pomocą otwarcia drzwi za pomocą ikonki z kłódką,
- **customized** – kod manualny – pozwala na pełne spersonalizowanie kodu dzięki możliwości wyboru czasu działania oraz numeru kodu (4-9 znaków),

UWAGA: W celu ustawienia kodu spersonalizowanego należy synchronizować aplikację z urządzeniem za pomocą Bluetooth.

- **cyclic** – kod cykliczny pozwala na ustawienie wg schematu, istnieje możliwość wyboru dnia tygodnia oraz godzin działania tego kodu – kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność.

3.5.3.2. Wygenerować kod klikając przycisk „Generate".

3.5.3.3. Kliknąć w ikonkę kwadracika ze strzałką znajdującą się w prawym górnym rogu aplikacji

3.5.3.4. Z listy wybrać metodę przesłania kodu:

- **SMS** – kod zostanie przesłany za pomocą wiadomości SMS – w wiadomości SMS pojawi się szablon z informacjami o kodzie dostępu, jego dacie ważności itp. - istnieje możliwość dowolnego edytowania wiadomości SMS
- **We chat**
- **Email**
- **Messenger**
- **Whatsapp**

} warunkiem wysłania wiadomości z kodem jest posiadanie skonfigurowanej aplikacji

3.5.4. **Attendance** – system uproszczonej rejestracji czasu pracy* – po aktywacji funkcji (patrz punkt 3.5.8) w menu głównym aplikacji pojawi się dodatkowa ikonka „Attendance".

3.5.4.1. **Ustawienie profilu firmy**

Po kliknięciu w ikonkę „Attendance" aplikacja przeniesie użytkownika do okna tworzenia profilu firmy „Create a Company", który niezbędny jest do rozpoczęcia rejestracji czasu pracy.

W celu konfiguracji konta należy uzupełnić pola:

- Company Name – nazwa firmy,
- Working Time – godziny pracy firmy:
  -- Starting Time - godzina otwarcia,
  -- Closing Time – godzina zamknięcia,
- Workday Setting – dni pracy firmy;
  -- Customized – ręczny wybór dni pracy od poniedziałku do niedzieli,
  -- One-Two Day weekend;
    --- This week – One day weekend – ustawienie 6-dniowego tygodnia pracy (wolna niedziela),
    --- This week – Two day weekend – ustawienie 5-dniowego tygodnia pracy (wolny weekend).

3.5.4.2. **Dodawanie pracowników do profilu firmy**

W celu dodania pracownika do profilu firmy należy kliknąć w ikonkę trybu znajdującą się w prawym górnym rogu aplikacji. Oprócz informacji wprowadzonych przy konfiguracji profilu firmy pojawią się dwa dodatkowe pola **- Staff** – personel oraz **Holiday** – święta (opcja pozwala ustawić dni, które mają zostać wyłączone z ewidencji czasu pracy).

Opcja Staff pozwala na dodanie profili pracowniczych, które mają podlegać obowiązkowi rejestracji czasu pracy. W celu dodania pracownika po wyborze opcji „Staff" należy kliknąć w ikonkę plusa znajdującą się w prawym górnym rogu aplikacji, po czym pojawi się nowe okno z funkcją dodania pracownika „**Add Staff**". W celu konfiguracji konta należy uzupełnić pola:

Name – Nazwa pracownika (np. imię i nazwisko)

Method – rodzaj weryfikacji czasu pracy:

- APP – użytkownik musi być posiadaczem konta w aplikacji TTLock

-- Already has eKey – użytkownik posiada już eKlucz:

--- Nie – należy wygenerować eKlucz - patrz punkt 3.5.2,

--- Tak – należy wybrać eKlucz z listy,

- Passcode – kod dostępu

-- Already has Passcode – użytkownik posiada kod dostępu

--- Nie – należy wcisnąć przycisk „Generate Passcode" i wygenerować kod

--- Tak – należy wybrać kod z listy

- IC Card – klucz zbliżeniowy (brelok Mifare 13,56 MHz)

-- Already has IC card – użytkwonik posiada brelok zbliżeniowy

--- Nie – należy kliknąć przycisk „Add IC Card" i dodać kartę – patrz punkt 3.5.6

--- Tak – należy wybrać brelok z listy

Po wprowadzeniu nazwy użytkownika i wyborze sposobu weryfikacji na liście „Straff" wyświetli się wprowadzona nazwa, po kliknięciu, której wyświetli się lista wprowadzonych informacji wraz z możliwości ich edycji. Ponadto z tego poziomu dostępny będzie wgląd w rejestr wejść i wyjść pracownika.

3.5.4.3. Wgląd w historię czasu pracy

Po sonfigurowaniu profilu firmy i dodaniu personelu, klikając w ikonkę „Attendence" dostępną w głównym menu aplikacji zobaczymy listę wszystkich pracowników. Po kliknięciu w danego pracownika może sprawdzić godzinę wejścia i wyjścia.

> ***Uwaga:** W z pozycji widoku kalendarza aplikacja wyświetla pierwsze wejście i ostatnie wyjście pracownika w danym dniu.
>
> Aby sprawdzić ilość wszystkich wejść i wyjść konkretnego pracownika w danym dniu należy wejść w zakładkę „Records" (dziennik logów) i odczytać historię wejść/wyjść danego użytkownika wpisując w wyszukiwarkę zdarzeń przypisaną mu nazwę.
>
> Aplikacja nie umożliwia generowania raportów przepracowanych godzin, dni itd.

3.5.4. **eKeys** – lista wygenerowanych i wysłanych kluczy dostępu – z informacjami o kluczach – rodzaj klucza, status aktywności – z pozycji listy możliwe jest usunięcie danego klucza, aby to zrobić należy przytrzymać palec na danym kluczu aż do pojawianie się przycisku „Delete" po jego naciśnięciu klucz zostanie trwale usunięty.

UWAGA: Usunięcie aktywnego klucza z listy w aplikacji przed czasem jego wygaśnięcia jest możliwe, aby tego dokonać urządzenie z aplikacją musi mieć dostęp do Internetu, a klucz zostanie usunięty dopiero, gdy osoba otrzymująca klucz również podłączy się do Internetu. Informacja o przedczasowym usunięciu klucza zostanie pobrana z serwera.

Z pozycji listy istnieje możliwość usunięcia wszystkich kluczy jednocześnie:
- należy kliknąć w ikonkę trzech kropek znajdującą się w prawym górnym rogu
- wybrać reset ekeys
- potwierdzić chęć zresetowania kluczy - wpisać hasło administratora aplikacji

3.5.5. **Passcodes** - lista wygenerowanych i wysłanych kodu dostępu – z informacjami o kodach – rodzaj, status aktywności – z pozycji listy możliwe jest usunięcie danego kodu, aby to zrobić należy przytrzymać palec na danym kodzie aż do momentu pojawianie się przycisku „Delete" po jego naciśnięciu klucz zostanie trwale usunięty.

UWAGA: Aby usunąć kod permanentny należy być w zasięgu nadajnika Bluetooth wbudowanego w szyld.

Z pozycji listy istnieje możliwość usunięcia wszystkich kodów jednocześnie:
- należy kliknąć w ikonkę trzech kropek znajdującą się w prawym górnym rogu,
- wybrać reset passcodes,
- potwierdzić chęć zresetowania kluczy - wpisać hasło administratora aplikacji.

3.5.6. **IC Cards** - szyldy z kontrolą dostępu posiadają wbudowany czytnik kart zbliżeniowych Mifare 13,56 Mhz, klikając w ikonkę IC Cards wchodzimy w panel zarządzania kartami dostępu.
Aby dodać kartę Mifare należy:
- kliknąć w ikonkę trzech kropek znajdującą się w prawym górnym rogu,
- wybrać opcję „add IC Cards",
- w polu „name" wpisać nazwę karty,
- wybrać rodzaj dostępu – permanentny lub czasowy,
- w przypadku wyboru dostępu czasowego należy ustawić termin ważności,
- kliknąć „OK" i czekać na sygnał z szyldu,
- po usłyszeniu komunikatu dźwiękowego przyłożyć kartę w okolicę cyfry"2" znajdującej się na klawiaturze numerycznej urządzenia.

Z pozycji listy istnieje możliwość usunięcia wszystkich kart jednocześnie:
- należy kliknąć w ikonkę trzech kropek znajdującą się w prawym górnym rogu,
- wybrać clear IC cards,
- potwierdzić chęć zresetowania kart - wpisać hasło administratora aplikacji.

UWAGA: Korzystając z opcji „Upload IC cards" istniejie możliwosc przesłania kopii zapasowej z listą dodanych kart na serwer.

3.5.7. **Records** – dziennik logów urządzenia

3.5.8. **Settings** – Ustawienia – klikając w ikonkę Settings mamy dostęp do informacji o urządzeniu:
- Lock Number – numer zamka
- MAC/ID - adres MAC/ nr ID
- Battery – status baterii
- Validitz Period – Ważność dostępu

- Lock Name - funkcja umożliwia wprowadzenie nazwy urządzenia
- Lock Group - funkcja umożliwia przypisania urządzenia na grupy
- Admin Passcode – funkcja umożliwia zmianę kodu administratora

- Lock Time – funkcja umożliwia synchronizację czasu urządzenia z czasem z aplikacji
- Auto Lock - funkcja umożliwia wprowadzenia długości impulsu (np. czasu zwalniania eletrozaczepu)
- Lock Sound - funkcja umożliwia włączanie/ wyłączanie dźwięków wydawanych przez klawiaturę urządzenia
- Unlock Remotly - funkcja umożliwia zdalne otwieranie zamka (aktywna wyłącznie w przypadku posiadania w systemie Bramki WiFi)
- Diagnosis – diagnozowanie problemów zamka
- Read Operation Recorde - wgląd w historię wszystkich operacji wykonywanych na urządzeniu
- Firmware Update – aktualizacja oprogramowania

- Attendance – Aktywacja uproszczonego systemu rejestracji czasu pracy (RCP)
- Unlock Notification – Informacje o odblokowaniu szyldu (prace aplikacji w tle)

- DELETE - funkcja usuwania zamka z aplikacji. Uwaga: Usunięcie urządzenia należy potwierdzić hasłem do konta na którym jesteśmy zalogowani w aplikacji.

UWAGA
W przypadku awarii i konieczności wysłania urządzenia do serwisu, uprzednio należy usunąć szyld z aplikacji TTlock.