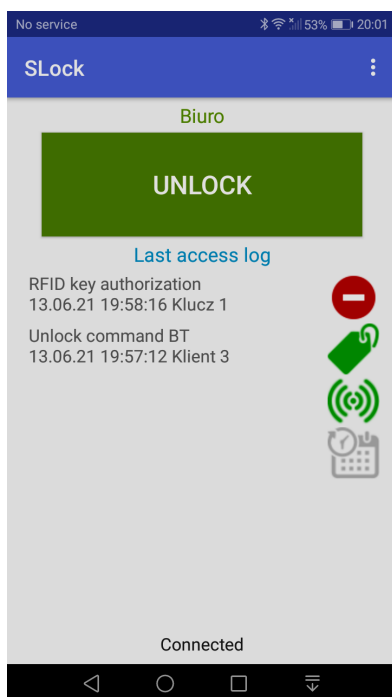


Aplikacja SLOCK

Do obsługi systemów kontroli dostępu
SmartKey i SmartLock



System SmartKey (SK) został zaprojektowany tak, aby maksymalnie uprościć jego budowę przy zachowaniu większości cech rozproszonych systemów stosowanych powszechnie w kontroli dostępu do pomieszczeń i budynków w odniesieniu do pojedynczego pomieszczenia / budynku / domu. System posiada również wersję do zastosowań motoryzacyjnych SmartLock (SL), będącą blokadą uruchomienia pojazdów silnikowych.

System obsługuje pojedyncze drzwi / bramę / furtę czy też schowek, skrytkę, sejf, itd., przy zastosowaniu zamka elektromechanicznego lub elektromagnetycznego (SK) lub elektroniczne / elektryczne urządzenia rozruchowe pojazdów samochodowych (SL).

System oprócz funkcji zabezpieczającej posiada szeroki zakres kontroli użytkowników, harmonogram oraz dziennik zdarzeń, co pozwala na kontrolę dostępu podobną do rozbudowanych (rozproszonych) i o wiele droższych systemów.

Bezpieczeństwo

Do jego obsługi przewidziana jest dedykowana aplikacja pracująca pod kontrolą systemu Android oraz zestaw kluczy RFID typu NTAG. Zastosowanie kluczy w postaci znaczników NTAG zabezpieczonych zestawem hasel wraz z odpowiednimi regułami bezpieczeństwa zaimplementowanymi w urządzeniu oraz przy stosowaniu zasad bezpieczeństwa dotyczących kart zbliżeniowych nie ustępuje poziomem zabezpieczenia kartom kryptograficznym, natomiast dla użytkownika są doskonałym wyborem ze względu na niski koszt można je dowolnie wymieniać, usuwać i zastępować innymi w przypadku naruszenia zasad bezpieczeństwa. Dodatkowym atutem jest fakt, że oprócz plastikowych kart NTAG użytkownik może stosować naklejane tagi RFID o tym samym poziomie zabezpieczeń.

Oprócz wykorzystania kluczy RFID do uzyskania dostępu można używać samej aplikacji SLock. Aplikacja poza kontrolą dostępu (analogicznie dokuczy RFID) zarządza całym systemem. System SLock posiada trzypoziomowe zabezpieczenie kodami ustalonymi indywidualnie dla każdego urządzenia przez administratora aplikacji.

1. Przed pierwszym użyciem

(dotyczy wszystkich nowych klientów)

Zanim zaczniesz używać aplikacji SLock, musisz dodać swoje urządzenie do listy sparowanych urządzeń w swoim telefonie. Kolejność czynności:

- *Podłącz zasilanie urządzenia SK/SL i poczekaj na uruchomienie*
- *Przytrzymaj przycisk serwisowy przez 3 sek. Zaświeci dioda LED (czerwona lub niebieska w zależności od rodzaju kontrolera), co oznacza wejście urządzenia w tryb odnajdywania (widoczności) BT Od tego czasu masz 120 sek na sparowanie urządzeń*
- *Wejdź w „Ustawienia” swojego telefonu, następnie „Urządzenia Bluetooth” i kliknij opcje „Szukaj” **
- *Po znalezieniu, na liście pojawi się urządzenie bluetooth „SmartKey” lub „SmartLock”*
- *Kliknij je i sparuj obydwa urządzenia*
- *Wprowadź domyślny kod parowania „00000000” (ten kod należy zmienić po zalogowaniu telefonu do urządzenia)*
- *Zaczekaj na zakończenie trybu odnajdywania – dioda LED zgaśnie, co oznacza powrót urządzenia SK/SL do normalnego trybu pracy*

*) Może się różnić w zależności od producenta i modelu telefonu

2. Pierwsze logowanie

(dotyczy wszystkich nowych klientów)

Pobierz i zainstaluj aplikację SLock, (jeśli nie zrobiłeś tego wcześniej). Kolejność czynności:

- *Uruchom aplikację – przy pierwszym uruchomieniu pojawi się komunikat „Brak pliku APP” jest to normalna sytuacja*
- *Wybierz z menu na pasku aplikacji „Ustawienia”*
- *W oknie ustawień wybierz z listy swoje urządzenie, następnie wprowadź kody PIN i ADM – odpowiednio domyślnie „0000” i „00000000” i zatwierdź*

- *Jeśli wszystko zrobiłeś poprawnie aplikacja połączy się i zaloguje się do urządzenia SK/SL*
- *Zamknij aplikację, aby zapisać wprowadzone dane*
- *Uruchom aplikację, zaloguj się ponownie do kontrolera i zmień kody dostępu PIN i ADM*

W przypadku pierwszego użycia należy po zmianie kodów dostępu PIN i ADM zmienić również kod parowania PAR

Zmiana kodów PIN, ADM i PAR w sekcji 3.1

3. Okno główne aplikacji

Podstawowym widżetem głównego okna jest przycisk „Odblokuj” wysyłający polecenie odblokowania zamka / zdjęcia blokady. Jeśli przycisk jest dostępny wyświetlany jest w kolorze zielonym, szary ciemny kolor oznacza, że urządzenie znajduje się w stanie odblokowania (zamek otwarty / blokada zdjęta). Poniżej znajduje się lista ostatnich czterech zdarzeń dotyczących poleceń odblokowania kluczami RFID oraz z poziomu aplikacji (wszystkie zdarzenia zawiera dziennik opisany w sekcji 3.5)

Prawa strona okna zawiera ikony stanu:

- stanu zamka (blokady)
- obecności czytnika kluczy RFID
- aktywności kluczy RFID
- aktywności harmonogramu kluczy

Dolna sekcja to okno komunikatów oraz panel szybkiego wyboru ostatnich urządzeń (pojawia się, kiedy w jednej aplikacji załogujesz się do więcej niż jednego urządzenia SK/SL)

3.1. Menu „Ustawienia”

Autoryzacja – tutaj należy wprowadzić kody dostępu PIN i ADM przed pierwszym logowaniem do nowego urządzenia.

Edycja kodów zabezpieczających – umożliwia zmianę kodów zabezpieczających PIN, ADM i PAR. Wybierz odpowiedni przycisk zmiany kodu i postępuj

według wyświetlanych poleceń. Każdy kod należy podać trzykrotnie – aktualny oraz 2 x nowy za każdym razem potwierdzając przyciskiem. Wyjątek stanowi zmiana kodu PAR, jako pierwszy należy wprowadzić aktualny kod ADM, następnie 2 x nowy kod PAR.

W przypadku zmiany kodu parowania, aplikacja zakończy połączenie z kontrolerem. Po ponowny nawiązaniu połączenia, system telefonu zażąda podania nowego kodu parowania. Kod ten można też nadać w sekcji „Ustawienia” -> „Bluetooth” swojego telefonu*, parując kontroler z telefonem jak przy pierwszym użyciu.

**) Może się różnić w zależności od producenta i modelu telefonu*

Pole edycji i przycisk „Zmień” – nadanie własnej nazwy urządzeniu (np. „Dom”, „Biuro”, „Auto”, itp.) Wybierz z listy swoje urządzenie, następnie wprowadź swoją krótką nazwę i wybierz przycisk „Zmień” oraz „Zastosuj”. Nazwa będzie widoczna tylko w aplikacji użytkownika, który ją wprowadził (nie dotyczy innych użytkowników)

Lista urządzeń Bluetooth – lista wszystkich urządzeń sparowanych z telefonem. Twoje urządzenia, do których załogowałeś się poprawnie przynajmniej jeden raz są wyświetlane z dodatkową przyjazną nazwą w nawiasach, którą możesz nadać jak opisano wyżej

Pole „Wibracje” – opcja potwierdzania poleceń wibracjami.

Jeżeli jesteś pierwszym użytkownikiem logującym się do urządzenia, musisz poprawnie wprowadzić obydwa kody PIN oraz ADM. Pozostali użytkownicy mogą podać tylko kod PIN (użytkownik) lub obydwa kody PIN i ADM (administrator) w ten sposób możesz decydować o uprawnieniach innych użytkowników.

3.2. Menu „Zarządzanie” (tylko ADM)

W tym oknie możesz zarządzać wszystkimi użytkownikami, decydując o dostępie bądź blokadzie użytkownika. Opcje te nie dotyczą użytkowników z uprawnieniami administratora, ich pola wyboru są nieaktywne i oznaczone dodatkowym znakiem „(A)”

Przyciskiem „Wyczyść” możesz usunąć listę wszystkich identyfikatorów użytkowników z pamięci urządzenia. Identyfikatory użytkowników mogą być tylko dodawane i nie jest możliwe usunięcie pojedynczego wpisu z pamięci urządzenia. Ta opcja czyści tablicę, co umożliwia usunięcie nieaktywnych i ponowne dodanie tylko aktualnych użytkowników urządzenia.

Opcja „Obsługa kluczy RFID” – aktywuje obsługę kluczy zbliżeniowych NTAG RFID

Opcja „Harmonogram” – aktywuje obsługę harmonogramu kluczy / użytkowników

Opcja „Monitor zasilania” (dla SmartKey) / „Tryb serwisowy” (dla SmartLock) – aktywuje podgląd zasilania awaryjnego (poziom naładowania akumulatora) lub aktywuje tryb serwisowy (blokad nieaktywna na czas oddania pojazdu do serwisu)

3.3. Menu „Klucze RFID” (tylko ADM)

Tutaj przeprowadzisz operacje programowania nowego klucza bądź usuwania lub niszczenia istniejących kluczy. Usunięcie klucza umożliwia jego ponowne zaprogramowanie, natomiast zniszczenie klucza uniemożliwia jego ponowne użycie w przyszłości (hasła na kluczu pozostają niezmienione, lecz są usuwane z pamięci urządzenia).

Programowanie – wybierz przycisk „Programuj” oraz „Zastosuj” zbliż klucz do czytnika, poczekaj na sygnał dźwiękowy i komunikat na ekranie smartfona

Usuwanie – wybierz przycisk „Usuń” oraz „Zastosuj” zbliż klucz do czytnika, poczekaj na sygnał dźwiękowy i komunikat na ekranie smartfona

Niszczenie – wybierz przycisk „Usuń” i „Zniszcz”, wybierz klucze do trwałego usunięcia, wybierz „Zastosuj”

Klucze oznaczone kolorem czerwonym są zablokowane. Sytuacja taka wystąpi po nieudanej autoryzacji klucza i może, (choć nie musi) oznaczać próbę włamania przy pomocy klucza z klonowanym nr seryjnym, lecz nieprawidłowymi hasłami. Klucz taki należy trwale usunąć, chyba, że istnieć pewność, iż winę ponosi sam użytkownik (patrz sekcja „jak używać kluczy RFID” w dokumencie „System SmartKey”)

3.4. Menu „Harmonogram” (tylko ADM)

Harmonogram umożliwia określanie przedziałów czasowych, w których dany użytkownik lub klucz będzie miał przyznane uprawnienia dostępu. Pojedynczy wpis harmonogramu obejmuje okres tygodnia w przedziałach godzinowych / dzień i jest ustalany razem dla użytkowników i kluczy. Maksymalnie można utworzyć cztery osobne wpisy harmonogramu oraz jeden wpis obejmujący „Zawsze uprawnione” (klucze i użytkownicy z tego wpisu mają ciągły dostęp w czasie aktywnego harmonogramu)

- *Dodawanie - Jeśli chcesz dodać nowy wpis wybierz dni tygodnia, klucze, użytkowników, godzinę początkową „Start” i końcową „Stop”, wybierz przycisk „Dodaj”*
- *Edycja - Jeśli chcesz edytować wpis, wybierz go z listy, wprowadź zmiany i wybierz „Zmień”*
- *Usuwanie - Jeśli chcesz usunąć wpis musisz usunąć wszystkie harmonogramy, wybierz „Wyczyść”*

Aby uaktywnić harmonogram, aktywuj opcję „Harmonogram” w menu „Zarządzanie”. Od teraz system będzie kontrolował dostęp według wpisów harmonogramu.

Przełącznik wyboru „Klucz” / „Klient” znajduje się na dole okna.

3.5. Menu „Dziennik”

W tym oknie znajduje się aktualizowany przy każdym jego otwarciu, podgląd dziennika zdarzeń (log). Po otwarciu tego okna należy zaczekać do zakończenia aktualizacji dziennika (wskazuje go pasek postępu). Dziennik posiada dwa poziomy filtrowania: 1) według źródła zdarzenia 2) według daty zdarzenia. Po wybraniu wpisu na liście zostanie aktywowany filtr 1) po ponownym wybraniu filtra 2). Przycisk systemowy telefonu „wstecz” cofa użycie ostatniego filtra.

3.5.1 Przycisk „Odśwież”

Przycisk ten po naciśnięciu pobiera ponownie ostatnie wpisy dziennika z kontrolera do pamięci telefonu, dłuższe przytrzymanie przycisku powoduje reset dziennika, wyczyszczenie pamięci logu w telefonie i

pobranie całości wpisów od nowa. Ta funkcja może pomóc w przypadku nieprawidłowej (zakłóconej) transmisji w czasie pobierania dziennika

3.5.2 Przycisk „Edytor nazw”

Edytor nazw – w tym oknie możesz nadać przyjazną, krótką nazwę dla użytkowników i kluczy zarejestrowanych w systemie, nazwy te będą widoczne na liście zdarzeń w dzienniku oraz w oknie głównym aplikacji tylko dla użytkownika aplikacji, który je wprowadził (nie dotyczą innych użytkowników)

Aby zmienić domyślną nazwę, wybierz wpis na liście, zmień nazwę w polu u góry okna zatwierdź przyciskiem „Zapisz”. Kiedy zmienisz wszystkie wybrane nazwy wybierz „Zastosuj”.

3.6. Menu „Informacje”

Okno wyświetla informacje dotyczące aplikacji w tym nr wersji oraz prawa autorskie. Dodatkowo w tym oknie znajduje się przycisk aktualizatora oprogramowania układowego (firmware), aktywny tylko wówczas, gdy urządzenie będzie wymagało takiej aktualizacji.

3.6.1 przycisk „Firmware” (tylko ADM)

Aktualizacja – upewnij się, że masz naładowaną baterię w smartfonie, jesteś w zasięgu urządzenia, a samo urządzenie ma stabilne zasilanie (nie zaleca się zasilania akumulatorowego w przypadku urządzenia SmartKey).

1. Wybierz przycisk „Połącz” nastąpi aktywacja bootloader’a procesora urządzenia, co zostanie potwierdzone zielonym napisem „Tryb bootloader’a aktywny”
2. Wybierz przycisk „Aktualizuj” rozpocznie się procedura aktualizacji firmware – zaczekaj do jej zakończenia
3. Po zakończeniu procedury urządzenie zostanie automatycznie zrestartowane
4. Wybierz przycisk „Zamknij” aplikacja zostanie zamknięta
5. Uruchom ponownie aplikację i zaloguj się do urządzenia.

Aktualizacja oprogramowania układowego jest szczególną operacją i należy ją przeprowadzać

świadomie i tylko wówczas, kiedy jest niezbędna. Przerwanie transmisji, zanik zasilania, utrata zasięgu, itp. spowoduje uszkodzenie oprogramowania wewnętrznego procesora i uniemożliwi normalne uruchomienie urządzenia (w takim przypadku musisz użyć trybu awaryjnego Bootloader – patrz instrukcja obsługi kontrolera pkt. 3.1).



Deklaracja zgodności UE
<https://dc-tech.pl/ce.html>



Aplikacja Slock w sklepie
Google Play:



Produkt zaprojektowany i wykonany w Polsce
© 2023 DK / DC-Tech