Polityka Prywatności

INTEGRA CONTROL to aplikacja mobilna i produkt uzupełniający przeznaczony dla rodziny central alarmowych **INTEGRA**. Został on stworzony przez **SATEL Sp. z o.o.** w celu zapewnienia naszym **Klientom** nowoczesnej i użytecznej aplikacji klienckiej umożliwiającej bezpieczny dostęp, zdalne sterowanie i wizualizację stanu centrali alarmowej zainstalowanej w obiekcie Klienta.

Aplikacja jest dostarczana przez SATEL Sp. z o.o. bezpłatnie i przeznaczona do użytku na zasadzie "tak jak jest".

Niniejsza strona zawiera informacje o polityce prywatności SATEL Sp. z o.o. dla naszych **Klientów**, którzy zdecydowali się na korzystanie z aplikacji. Polityka prywatności jest również dostępna w aplikacji mobilnej INTEGRA CONTROL.

Podjęcie decyzji o korzystaniu z aplikacji oznacza wyrażenie zgody na zbieranie i wykorzystywanie przez nas informacji związanych z niniejszą polityką prywatności. **Informacje**, które zbieramy służą dostarczaniu i udoskonalaniu aplikacji. Informacji o klientach nie udostępniamy nikomu, ani nie używamy do żadnych innych celów poza opisanymi w niniejszej polityce prywatności.

Gromadzenie i wykorzystywanie informacji

Istnieją dwa sposoby realizacji komunikacji typu "end-to-end" pomiędzy aplikacją INTEGRA CONTROL a centralą alarmową:

Przypadek 1: Bezpośrednie połączenie sieciowe P2P,

Przypadek 2: Pośrednie połączenie sieciowe realizowane za pośrednictwem serwerów komunikacyjnych.

W obu przypadkach komunikacja między centralą alarmową a klientem/klientami aplikacji mobilnej jest realizowana poprzez sieć przy użyciu bezpiecznych protokołów transportowych.

W przypadku pośredniego połączenia sieciowego komunikacja typu "end-to-end" jest również realizowana z wykorzystaniem bezpiecznych usług transmisji danych hostowanych na specjalnych serwerach komunikacyjnych, należących do i utrzymywanych przez SATEL Sp. z o.o.

Podjęcie decyzji o zastosowaniu aplikacji do uzyskania zdalnego połączenia i wizualizacji stanu systemu alarmowego Klienta oznacza zgodę na inicjalizację aplikacji klienckiej z wykorzystaniem następujących informacji:

Przypadek 1: Bezpośrednie połączenie sieciowe P2P

Adres IP lub **adres URL** reprezentujący daną centralę alarmową, **PORT** komunikacyjny, **hasło użytkownika** reprezentujące konto użytkownika w danej centrali alarmowej oraz **klucz GuardX** potrzebny do otwarcia kanału komunikacji z centralą alarmową. Taki zestaw danych jest wprowadzany w aplikacji i przechowywany w jej zasobach lokalnie w urządzeniu

użytkownika. Jest to zestaw danych wystarczający do nawiązania połączenia z centralą alarmową.

Przypadek 2: Pośrednie połączenie sieciowe realizowane przez serwery komunikacyjne.

Adres MAC, **identyfikator** centrali alarmowej, **hasło użytkownika** reprezentujące konto użytkownika w danej centrali alarmowej oraz **klucz GuardX** potrzebny do otwarcia kanału komunikacji z centralą alarmową. Taki zestaw danych jest wprowadzany w aplikacji i przechowywany w jej zasobach lokalnie w urządzeniu użytkownika. Jest to zestaw danych wystarczający do nawiązania połączenia z centralą alarmową.

Objaśnienia:

- **Adres IP** lub **adres URL** i **PORT** reprezentują komunikację z daną centralą alarmową i identyfikację centrali alarmowej w sieci.
- **Adres MAC** to identyfikator przypisywany centrali alarmowej podczas procesu produkcyjnego. Służy on do identyfikacji danego urządzenia w sieci i w naszym systemie. Jest podany w sposób jawny na tabliczce znamionowej urządzenia
- **Identyfikator** centrali alarmowej jest generowany przez nasze serwery i przypisywany do urządzenia podczas żądania i inicjalizacji połączenia między centralą alarmową a serwerem. Identyfikator jest przechowywany w sposób zabezpieczony. Można go pobrać za pomocą funkcji użytkownika dostępnych w centrali alarmowej po poprawnym uwierzytelnieniu użytkownika
- **Hasło użytkownika** jest znane tylko danemu użytkownikowi i jego centrali alarmowej. Hasło to jest potrzebne, aby uzyskać dostęp do konta użytkownika w centrali alarmowej. Nie jest to informacja niezbędna, lecz bez jej wprowadzenia Klient nie będzie miał dostępu do funkcji związanych ze swoim kontem. Klient będzie miał tylko dostęp do manipulatora wirtualnego, który posiada taką samą funkcjonalność co manipulator fizyczny zainstalowany w systemie alarmowym.
- **Klucz GuardX** jest kluczem prywatnym, zdefiniowanym przez administratora centrali alarmowej podczas konfigurowania kanału komunikacji. Klucz ten jest przechowywany w pamięci centrali alarmowej. Można go odzyskać za pomocą dedykowanej funkcji serwisowej dostępnej tylko w trybie serwisowym centrali alarmowej lub specjalnego programu o nazwie DLOADX służącego do konfiguracji systemu alarmowego. Po stronie aplikacji klucz musi być wprowadzony ręcznie przez użytkownika.

Uwaga: Satel Sp. z o.o. nie posiada kompletnego zestawu danych, który pozwoliłyby na połączenie z centralą alarmową konkretnego użytkownika. Po stronie Klienta powyższy zestaw danych jest przechowywany w zasobach aplikacji w urządzeniu Klienta. Ponadto w aplikacji można ustawić hasło, które będzie używane do weryfikacji praw dostępu do aplikacji i do danych przechowywanych w zasobach aplikacji.

Nawiązanie komunikacji typu "end-to-end" oznacza ciągłą transmisję zabezpieczonych danych z central alarmowych do aplikacji klienckiej w celu wymiany konfiguracji systemu alarmowego i uzyskania informacji o stanie systemu alarmowego za pomocą funkcji sprawdzania stanu systemu, sprawdzania stanu wejść, sprawdzania stanu wyjść, przeglądania awarii bieżących i przeglądania wszystkich zdarzeń systemowych.

SATEL Sp. o.o. nie zbiera żadnych danych związanych z komunikacją typu "end-to-end". Dane są przechowywane tylko w urządzeniu komunikacyjnym Klienta i w aplikacji mobilnej. Nasze serwery reprezentują jedynie warstwę transportową.

Podjęcie decyzji o aktywacji powiadomień PUSH w aplikacji klienckiej oznacza zgodę na pobieranie przez nas identyfikatora urządzenia, w którym aplikacja jest zainstalowana i wykorzystywanie go do świadczenia usługi powiadomień PUSH. Tokeny oznaczające instancje korzystania z usługi PUSH przez aplikację są przechowywane w bazach danych naszych serwerów. Konfiguracja usługi PUSH jest przechowywana w pamięci podręcznej aplikacji. Przy pomocy tych danych SATEL Sp. z o.o. nie jest w stanie zidentyfikować Klienta.

Nasza aplikacja wykorzystuje kody QR, aby ułatwić import danych potrzebnych do inicjalizacji połączenia z centralą alarmową. Ta sama funkcja służy do eksportu danych z centrali alarmowej do innych instancji aplikacji w innym urządzeniu.

Podjęcie decyzji o korzystaniu z naszej aplikacji do skanowania kodu QR i imporcie danych centrali alarmowej za pomocą kodu QR oznacza zgodę na korzystanie z kamery danego urządzenia. Należy pamiętać, że nasza aplikacja wykorzystuje kamerę wyłącznie do odczytu kodu QR.

Dane użytkownika zawarte w kodzie QR nie są przedstawione w sposób jawny. Kod QR jest generowany raz podczas sesji wymiany i zabezpieczony kluczem sesyjnym. Klucz sesyjny jest zdefiniowany przez użytkownika i nie jest wymieniany w naszej aplikacji. Podczas odczytywania kodu QR za pomocą aplikacji w urządzeniu docelowym użytkownik jest proszony o podanie dokładnego klucza sesyjnego.

Nasza aplikacja nie korzysta z usług innych firm, które mogą zbierać informacje używane do identyfikacji użytkownika. Nasza aplikacja nie korzysta i nie gromadzi żadnych danych, które mogą być uznane za wrażliwe.

Dane rejestru zdarzeń i analityka

Podjęcie decyzji o korzystaniu z naszej aplikacji oznacza zgodę na stosowanie przez nas technologii analitycznych **Google Analytics** i **Crashlytics** (część firmy Fabric zakupionej przez Google). Aby dowiedzieć się więcej o polityce prywatności Google Analytics's, odwiedź stronę http://www.google.com/analytics/learn/privacy.html. Aby dowiedzieć się więcej o polityce prywatności Crashlytics, odwiedź stronę: http://try.crashlytics.com/terms/

Powyższe technologie stosujemy do zbierania anonimowych danych, aby lepiej zrozumieć w jaki sposób użytkownik korzysta z naszej aplikacji. Dzięki tym narzędziom dowiadujemy się jak ulepszyć jej obsługę i które z jej funkcji są używane. Dostarczają nam one również ogólnych informacji o tym, gdzie na świecie nasza aplikacja jest wykorzystywana i jakiej wersji językowej nasi Klienci używają.

Informujemy, że w przypadku wystąpienia jakiegokolwiek błędu podczas pracy użytkownika z aplikacją, firma Crashlytics może przetwarzać raporty o błędach zapisanych w rejestrze zdarzeń danego urządzenia. Dane rejestru zdarzeń mogą zawierać np. nazwę urządzenia, wersję systemu operacyjnego, wersję aplikacji, czas i datę korzystania z aplikacji. Dane

rejestru zdarzeń są zbierane tylko po to, aby umożliwić nam rozwój i doskonalenie naszej aplikacji.

Pliki typu "cookies"

Cookies to pliki z małą ilością danych, które mogą zawierać anonimowy niepowtarzalny identyfikator. Są one przesyłane do przeglądarki Klienta z odwiedzanej przez niego strony internetowej i przechowywane w pamięci wewnętrznej urządzenia Klienta.

Nasza witryna internetowa wykorzystuje cookies w celu gromadzenia informacji i poprawy jakości usług. Użytkownik ma możliwość zaakceptowania lub odrzucenia cookies, oraz dowiedzenia się kiedy plik cookie jest wysyłany do komputera Klienta. W przypadku odrzucenia naszych plików cookies, niektóre części naszego serwisu mogą być dla użytkownika niedostępne.

Aplikacja INTEGRA CONTROL nie zawiera łączy do żadnej z naszych stron internetowych i dlatego nie wykorzystuje plików cookies.

Linki do innych stron

Aplikacja INTEGRA CONTROL nie posiada żadnych łączy URL.

Bezpieczeństwo

Cenimy sobie zaufanie Klientów dostarczających nam dane, o których mowa w niniejszej polityce prywatności i dlatego staramy się stosować komercyjnie akceptowalne środki ochrony. Należy jednak pamiętać, że żadna metoda przesyłu przez Internet, ani ich elektronicznego przechowywania nie jest w 100% bezpieczna i niezawodna, nie możemy więc zagwarantować ich absolutnego bezpieczeństwa.

Zmiany w niniejszej polityce prywatności

Nasza polityka prywatności może być od czasu do czasu aktualizowana, zalecamy więc okresowe śledzenie niniejszej strony pod kątem zmian. O wszelkich zmianach będziemy informować Klientów poprzez opublikowanie na niniejszej stronie nowej polityki prywatności. Zmiany takie wchodzą w życie natychmiast po ich zamieszczone na stronie internetowej.

Kontakt

W przypadku jakichkolwiek pytań lub sugestii dotyczących naszej polityki prywatności, prosimy o kontakt:

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk, Poland
satel@satel.pl

Made to Protect
http://www.satel.eu/