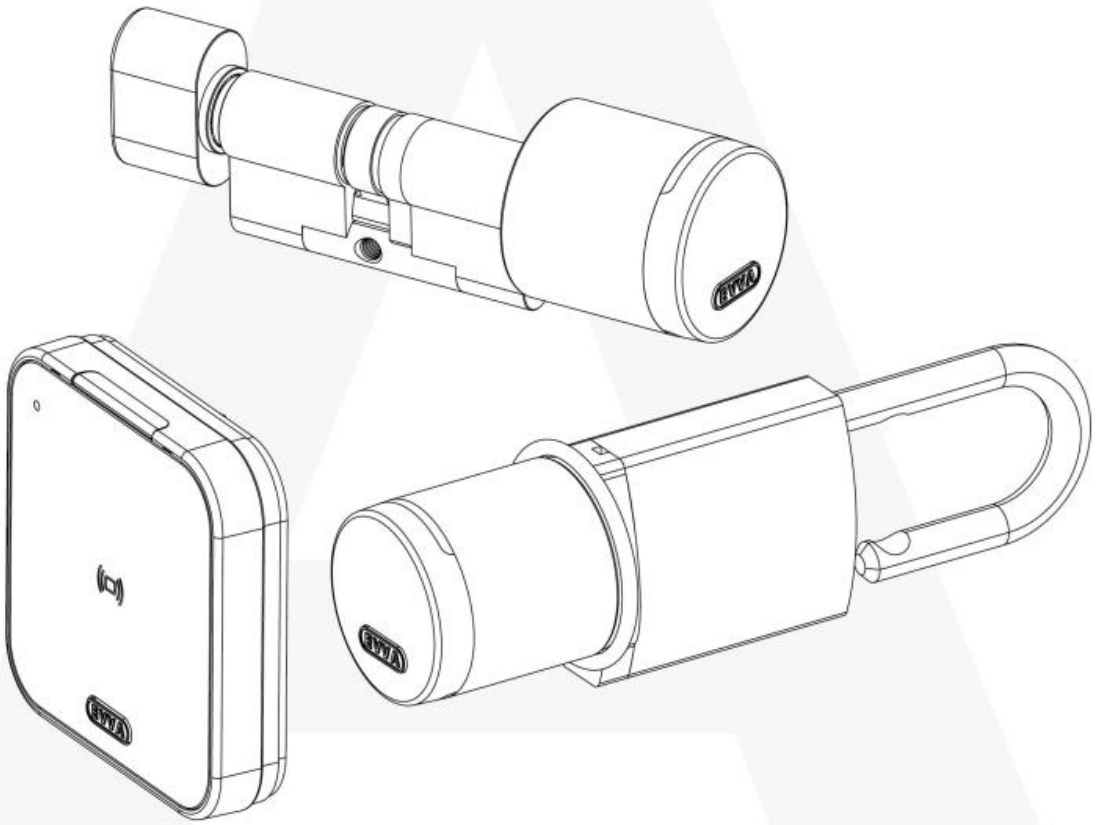


AirKey

Podręcznik systemu 2.6

1 Spis treści

2 Wprowadzenie, przegląd

Niniejszy podręcznik systemu AirKey zawiera informacje dotyczące instalacji, eksploatacji i obsługi elektronicznego systemu zamknięć AirKey, składającego się z modułu zarządzania online, aplikacji, wkładek i czytników naściennych, kłódek oraz nośników dostępu AirKey.

Produkty lub oprogramowanie użytkownika (Moduł zarządzania online systemu AirKey), które opisano w podręczniku systemu AirKey, może obsługiwać wyłącznie personel posiadający odpowiednie kwalifikacje do realizacji określonych zadań. Wykwalifikowany personel na podstawie posiadanych wiadomości i umiejętności jest w stanie rozpoznać niebezpieczeństwa powstające w wyniku obsługi tych produktów/systemów, a także unikać możliwych zagrożeń.

2.1 Ogólne wskazówki prawne

- Firma EVVA zawiera umowę o użytkowanie systemu AirKey wyłącznie w oparciu o swoje Ogólne Warunki Handlowe (EVVA-OWH) oraz Ogólne Warunki Licencyjne (EVVA-OWL) w odniesieniu do oprogramowania dla produktu.
- Nabywca jest jednoznacznie poinstruowany, że stosowanie objętego umową systemu zamknięć może wywołać skutki ustawowe, zwłaszcza w zakresie obowiązków dotyczących zezwoleń, zgłoszeń i rejestracji odnośnie prawa ochrony danych (np. wspólny system informacyjny), a także w przypadku stosowania w przedsiębiorstwie może wystąpić prawo do współdecydowania przez personel. Za zgodne z prawem zastosowanie produktu odpowiada nabywca lub klient i użytkownik końcowy.
- Zgodnie z odpowiedzialnością cywilną producenta za swoje produkty, zdefiniowaną w austriackiej ustawie o odpowiedzialności cywilnej za produkty wadliwe, należy przestrzegać powyższych informacji i przekazać je operatorom i użytkownikom. Niestosowanie się do niniejszej instrukcji zwalnia firmę EVVA z odpowiedzialności cywilnej.
- Produkt nie jest odpowiedni dla dzieci w wieku poniżej 36 miesięcy z uwagi na niebezpieczeństwo uduszenia spowodowanego przez połknięcie małych części.
- Niezgodne z umową lub nadzwyczajne zastosowanie, prace naprawcze lub modyfikacje, które nie zostały jednoznacznie dopuszczone przez firmę EVVA, a także niefachowy serwis mogą prowadzić do usterek w działaniu i nie należy ich wykonywać. Wszelkie zmiany, które nie zostały jednoznacznie dopuszczone przez firmę EVVA, powodują utratę wszelkich uprawnień wynikających z odpowiedzialności cywilnej, gwarancyjnej i innych możliwych oddzielnych uzgodnień gwarancyjnych.
- Architekci oraz doradcy budowlani są zobowiązani do pobrania od firmy EVVA wszystkich koniecznych informacji o produkcie zgodnie z wymogami austriackiej ustawy o odpowiedzialności cywilnej za produkty wadliwe. Sprzedawcy i technicy powinny przestrzegać wskazówek zawartych w dokumentacji firmy EVVA i ewentualnie przekazać je swoim klientom.
- Podczas projektowania i instalowania komponentów zamykających należy uwzględnić odpowiednie międzynarodowe i krajowe wytyczne wynikające z określonych ustaw, rozporządzeń, norm i dyrektyw, szczególnie w odniesieniu do wymogów w zakresie dróg ewakuacyjnych i wyjść awaryjnych.

2.2 Wsparcie techniczne EVVA

System AirKey to dopracowany i sprawdzony system zamknięć. Jeśli jednak zajdzie potrzeba skorzystania ze wsparcia, należy zwrócić się do partnera firmy EVVA.

Listę certyfikowanych partnerów firmy EVVA można znaleźć na firmowej stronie internetowej pod adresem: https://www.evva.com/pl-pl/wyszukaj-sprzedawce/.

Po wybraniu opcji filtrowania "Partner - Elektronika" można wykonać docelowe wyszukiwanie partnerów EVVA, którzy dystrybuują elektroniczne systemy zamknięć EVVA i dysponują odpowiednimi kwalifikacjami w tym zakresie.

W przypadku określonych zapytań należy skorzystać z udostępnionego formularza online. Formularz online został przewidziany do użytku w razie następujących sytuacji:

- Przekroczono maksymalną liczbę prób wprowadzania kodu przy użyciu nieprawidłowego kodu kredytu.
- Nie można załadować kredytu.
- Strona logowania Modułu zarządzania online systemu AirKey jest niedostępna.
- Logowanie jest niemożliwe Użytkownik nie pamięta swojego identyfikatora i/lub adresu e-mail.
- Uaktywniłeś uwierzytelnianie dwuetapowe i nie masz dostępu do swojego numeru telefonu.

Formularz online można znaleźć na stronie https://www.evva.com/pl/airkey/support/.

Informacje ogólne na temat systemu AirKey znajdują się na stronie pod adresem: https://www.evva.com/pl/airkey/website/.

2.3 Objaśnienie symboli

Ciąg poleceń, poszczególne polecenia lub przyciski zaprezentowano w niniejszym podręczniku systemu w poniższy sposób.

Przykład: Menu główne ***Nośniki i osoby*** → ***Utwórz osobę*** lub przyciski takie jak np. ***Zapisz***.

Uwaga – niebezpieczeństwo szkód rzeczowych, jeśli nie zostaną zachowane odpowiednie środki ostrożności.

Wskazówki i dodatkowe informacje

Porady i zalecenia

Komunikaty błędu

Option Opcje

2.4 Wskazówki dotyczące optymalnej nawigacji w tym dokumencie

W tym dokumencie znajduje się również wiele linków wewnętrznych, które prowadzą do innych rozdziałów lub fragmentów tekstu. Najszybszym i najwygodniejszym sposobem powrotu do oryginalnego miejsca w systemie Windows lub do przodu jest skorzystanie z tych **kombinacji przycisków**:

Alt + ◄ (Alt + strzałka kursora w lewo) = przejście do tyłu

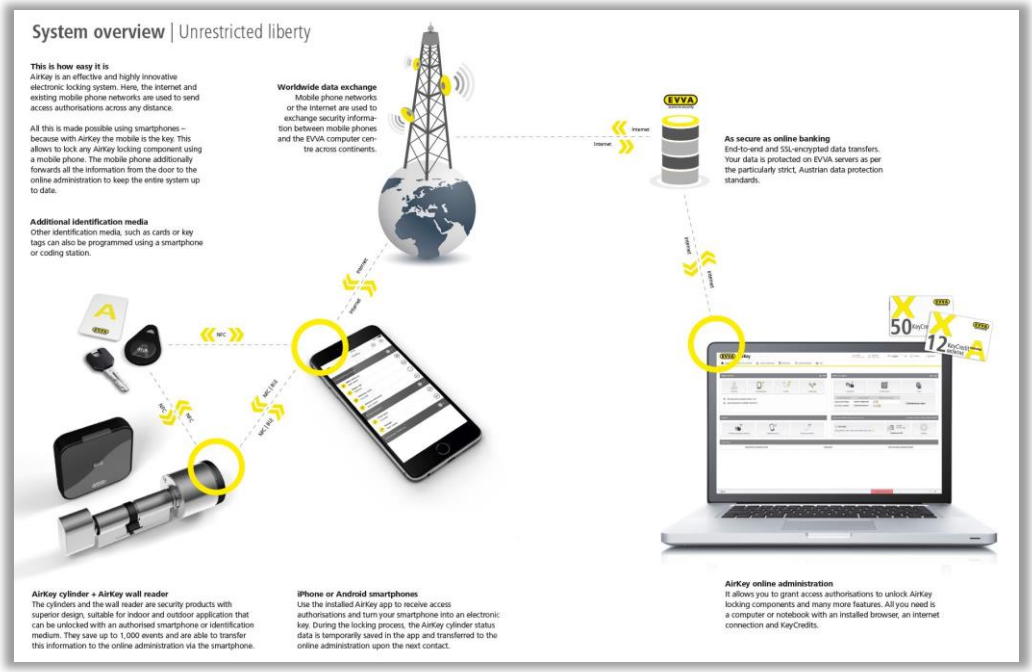
Alt + ► (Alt + strzałka kursora w prawo) = poruszaj się do przodu

Kombinacje klawiszy działają w wielu przeglądarkach PDF, np. Microsoft Word.

Aby wypróbować skróty klawiaturowe, kliknij ten link i wróć Alt + ◄ za pomocą przycisku.

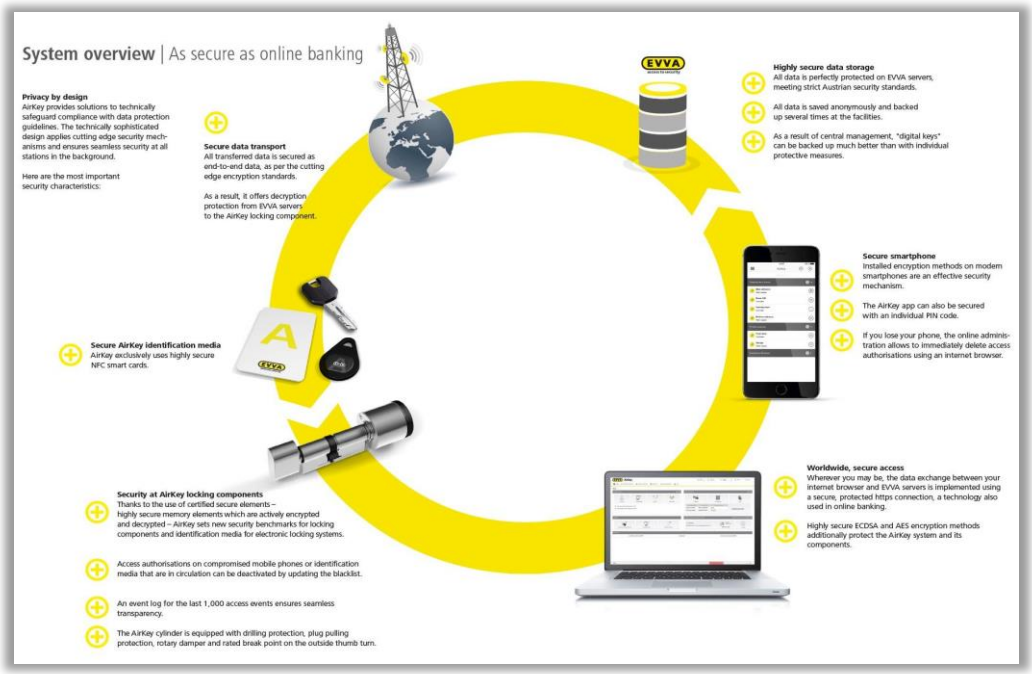
3 Architektura systemu

Poniższa ilustracja zawiera przegląd komponentów zastosowanych w systemie AirKey oraz ich powiązania komunikacyjne. Poszczególne komponenty opisano w kolejnej części dokumentu.



Rys. 1: Architektura systemu

Wszystkie dane są transmitowane w trybie end-to-end, zgodnie z aktualnymi standardami szyfrowania. Dane są szyfrowane na ścieżce komunikacyjnej od centrum obliczeniowego EVVA aż do komponentu zamykającego.



Rys. 2: Przegląd systemu – kompletne bezpieczeństwo

3.1 Komponenty zamykające

Komponenty zamykające (wkładki i czytniki naścienne AirKey) regulują dostęp do drzwi. W zależności od uprawnienia następuje odblokowanie lub odmowa dostępu realizowana przez komponent zamykający.

3.1.1 Wkładka AirKey

Wkładka AirKey to komponent zamykający zasilany baterią. Nadaje się do zastosowań wewnętrznych i zewnętrznych. W zależności od określonych wymagań wkładkę AirKey można także stosować w strefach istotnych dla bezpieczeństwa. Wkładka AirKey jest zabezpieczona mechanicznie przed aktami wandalizmu i manipulacją. Wkładkę AirKey można stosować w drzwiach przeciwpożarowych i ewakuacyjnych* przy uwzględnieniu wytycznych określonych w normach.

Wkładka AirKey jest dostępna jako półwkładka lub wkładka dwustronna. Wkładka dwustronna jest dostępna jako model z dostępem jednostronnym lub obustronnym. W przypadku modelu z dostępem jednostronnym elektroniczna kontrola uprawnień jest realizowana na zewnątrz, a w przypadku modelu z dostępem obustronnym – po stronie wewnętrznej i zewnętrznej. Elektroniczna gałka po stronie z funkcją identyfikacji obraca się swobodnie w razie braku uprawnień. Czarny element z tworzywa sztucznego, osadzony na wkładce AirKey, służy jako czytnik.

Jeśli użytkownik przytrzyma przy gałce uprawniony nośnik, wkładka zostanie zasprzęglona przez określony czas i poprzez obrócenie gałki możliwe będzie otwarcie zamka. W tym zakresie należy przestrzegać także wskazówek zawartych w rozdziale Obsługa komponentów zamykających AirKey.

Należy pamiętać, że po zamknięciu drzwi nie następuje ich automatyczne ryglowanie. Blokowanie drzwi należy wykonać ręcznie lub alternatywnie za pomocą odpowiedniego dodatkowego urządzenia.

Należy sprawdzić, czy wybrana wkładka AirKey nadaje się do przewidzianego zastosowania. W tym celu wkładka AirKey jest dostępna w różnych formach konstrukcyjnych i konfiguracjach.

Niezbędne w tym celu arkusze specyfikacji oraz katalog produktu są dostępne w sekcji materiałów do pobrania na naszej stronie domowej https://www.evva.com/pl/downloads/.

Wkładka AirKey jest wyposażona w sygnalizację optyczną i akustyczną. Objaśnienie różnych sygnałów można znaleźć w rozdziale Sygnalizacja komponentów zamykających.

* W razie użytku w drzwiach ewakuacyjnych i antypanicznych może być konieczne zastosowanie funkcji antypanicznej FAP (w zależności od użytego zamku wpuszczanego). W tym zakresie należy przestrzegać odpowiednich wskazówek lub certyfikatów producentów zamków oraz kodu produktu podczas składania zamówienia.

Podczas montażu wkładki AirKey należy przestrzegać dołączonej do opakowania instrukcji montażowej lub wskazówek zawartych w filmie na temat montażu, udostępnionym pod adresem https://www.evva.com/pl/airkey/website/.

3.1.2 Wkładka hybrydowa AirKey

Wkładka hybrydowa AirKey ma identyczne właściwości jak wkładka AirKey. Dzięki temu nadaje się ona do zastosowań wewnętrznych i zewnętrznych a także w strefach istotnych dla bezpieczeństwa.

W porównaniu z wkładką podwójną AirKey z jednostronnym dostępem we wkładce hybrydowej AirKey po wewnętrznej stronie zamiast gałki mechanicznej znajduje się moduł do klucza. Tak więc dostęp od zewnątrz odbywa się na podstawie elektronicznej kontroli uprawnień a od wewnątrz kluczem mechanicznym.

Należy pamiętać, że po zamknięciu drzwi nie następuje ich automatyczne ryglowanie. Blokowanie drzwi należy wykonać ręcznie lub alternatywnie za pomocą odpowiedniego dodatkowego urządzenia.

Należy dokładnie sprawdzić, czy wkładka hybrydowa AirKey nadaje się do przewidzianego zastosowania.

Potrzebny do tego celu arkusz specyfikacji można pobrać z naszej strony firmowej w sekcji materiałów do pobrania: https://www.evva.com/pl/downloads/.

Wkładka hybrydowa AirKey jest wyposażona w sygnalizację optyczną i akustyczną. Objaśnienie różnych sygnałów można znaleźć w rozdziale Sygnalizacja komponentów zamykających.

Podczas montażu wkładki hybrydowa AirKey należy przestrzegać dołączonej do opakowania instrukcji montażowej.

3.1.3 Zamki gwintowane z ryglem AirKey

Zamki gwintowane z ryglem AirKey to komponent zamykający zasilany na baterię do zastosowań w garderobach, witrynach, różnych pojemnikach a także do zewnętrznych i wewnętrznych skrzynek pocztowych.

Po stronie zewnętrznej dostęp odbywa się na podstawie elektronicznej kontroli uprawnień. Po stronie wewnętrznej znajduje się rygiel do ryglowania. Zarówno odryglowanie jak i ryglowanie może być wykonywane dopiero po pozytywnym wyniku kontroli uprawnień, przez ręczne obrócenie zamka gwintowanego z ryglem AirKey. Inaczej niż w przypadku wkładki AirKey i wkładki hybrydowej, gałka elektroniczna po stronie identyfikacji nie obraca się swobodnie w razie braku uprawnień.

Sprawdź, czy zamek gwintowany z ryglem AirKey nadaje się do przewidywanego zastosowania. Zamek gwintowany z ryglem AirKey jest dostępny w wielu różnych formach konstrukcyjnych i konfiguracjach.

Potrzebny do tego celu arkusz specyfikacji można pobrać z naszej strony firmowej w sekcji materiałów do pobrania: https://www.evva.com/pl/downloads/.

Zamki gwintowane z ryglem AirKey jest wyposażona w sygnalizację optyczną i akustyczną. Objaśnienie różnych sygnałów można znaleźć w rozdziale Sygnalizacja komponentów zamykających.

Podczas montażu zamki gwintowane z ryglem AirKey należy przestrzegać dołączonej do opakowania instrukcji montażowej.

3.1.4 Kłódka AirKey

Kłódka AirKey to komponent zamykający z zasilaniem bateryjnym do stosowania w systemach szlabanów, rolet, magazynów i kontenerów archiwizacyjnych w zastosowaniach zewnętrznych i wewnętrznych.

Dostęp odbywa się na podstawie elektronicznej kontroli uprawnień na spodzie. Do ryglowania służy pałąk z hartowanej stali. Zarówno odryglowanie jak i zaryglowanie może nastąpić dopiero po kontroli uprawnień, przez ręczne obracanie gałką elektroniczną kłódki AirKey.

Sprawdź, czy kłódka AirKey nadaje się do planowanego zastosowania. Kłódka AirKey jest dostępna w różnych konfiguracjach.

Potrzebny do tego celu arkusz specyfikacji można pobrać z naszej strony firmowej w sekcji materiałów do pobrania: https://www.evva.com/pl/downloads/.

Kłódka AirKey jest wyposażona w sygnalizację optyczną i akustyczną. Objaśnienie różnych sygnałów można znaleźć w rozdziale Sygnalizacja komponentów zamykających.

Podczas montażu kłódka AirKey należy przestrzegać dołączonej do opakowania instrukcji montażowej.

Narzędzie montażowe do wkładki AirKey, wkładka hybrydowa, zamek gwintowany z ryglem i kłódka

Wkładka AirKey, zamki gwintowane z ryglem, wkładka ryglowana, i kłódka zapewniają ochronę mechanizmu specjalnego przed manipulacją. Gałkę elektroniczną można zdjąć wyłącznie za pomocą specjalnego narzędzia. Narzędzie montażowe potrzebne do montażu, demontażu i wymiany baterii nie jest standardowo dołączane do wkładki AirKey i dlatego należy zamawiać je osobno.

Kod zamówienia znajdziesz w katalogu produktu AirKey w sekcji materiałów do pobrania pod adresem https://www.evva.com/pl/downloads/.

3.1.5 Czytnik naścienny AirKey

Czytnik naścienny AirKey można stosować w obszarze wewnętrznym, zewnętrznym, w wersji pod- i natynkowej, a także w strefach istotnych dla bezpieczeństwa.

W obszarach zewnętrznych lub mokrych, a także w przypadku montażu podtynkowego należy stosować przewidzianą do tego celu, dołączoną do produktu uszczelkę. Należy także przestrzegać wskazówek zawartych w instrukcji montażowej.

Czytnik naścienny AirKey jest połączony z centralką sterującą AirKey za pomocą kabla CAT5 (maks. 100 m, Loop maks. = 2 Ohm), służącego także do zasilania czytnika. Centralka sterująca AirKey jest zasilana przez zasilacz i w razie awarii w dopływie prądu dysponuje buforem danych na okres maks. 72 h, o ile centralka sterująca AirKey była wcześniej eksploatowana przez co najmniej 6 godzin.

Należy pamiętać, że jeden czytnik naścienny AirKey można eksploatować w połączeniu z jedną centralką sterującą AirKey.

Za pośrednictwem kombinacji centralki sterującej i czytnika naściennego AirKey można sterować elektronicznymi elementami zamykającymi, takimi jak wkładki motoryczne, drzwi rozwierane, przesuwne itp.

Do centralki sterującej można również podłączyć zewnętrzne urządzenie udostępniające (przycisk). Po jego naciśnięciu drzwi zostaną otwarte, tak jak w przypadku dostępu za pośrednictwem modułu czytnika. Jednak otwarcie drzwi dokonane za pomocą zewnętrznego urządzenia udostępniającego NIE będzie protokołowane. Ze względów bezpieczeństwa należy wziąć pod uwagę, że w ten sposób za pomocą obcego systemu można uzyskać dostęp do systemu AirKey, przy czym nie nastąpi utworzenie wpisu w protokole dostępów.

Należy dokładnie sprawdzić, czy wybrany produkt AirKey nadaje się do przewidzianego zastosowania/sytuacji montażowej. Potrzebną do tego celu informację lub instrukcję montażu można pobrać z naszej strony firmowej https://www.evva.com/pl/downloads/.

3.2 Aplikacja AirKey

Aplikacja AirKey jest udostępniona przez firmę EVVA i można ją bezpłatnie pobrać z witryny Google Play Store lub Apple App Store.

Aplikacja AirKey jest niezbędna do obsługi komponentów zamykających AirKey za pomocą smartfona. Ponadto smartfon może także służyć do dodawania komponentów zamykających i nośników do systemu zamknięć AirKey, a także do ich aktualizacji. Aby korzystać z większości funkcji aplikacji AirKey, niezbędny jest dostęp do Internetu. Wyjątkiem jest tutaj uruchomienie komponentów zamykających.

Połączenie z Internetem może odpowiednio generować dodatkowe koszty. Należy uwzględnić obowiązującą taryfę opłat w tym zakresie.

3.3 Smartfony

Smartfon, który będzie stosowany w ramach systemu AirKey, powinien spełniać następujące wymagania minimalne:

- Obsługa technologii NFC lub Bluetooth 4.0 (Bluetooth Low Energy/BLE)
- System operacyjny:
  - Android™ w wersji 5.0 lub nowszej (możliwość obsługi wyłącznie technologii NFC)
  - Android™ w wersji 6.0 lub nowszej (możliwość obsługi NFC i Bluetooth)
  - Apple™ w wersji iOS 10 lub nowszej (możliwość obsługi wyłącznie technologii Bluetooth)
- Aplikacja AirKey z witryny Google Play Store lub Apple App Store
- Smartfony z systemem Android wymagają uprawnienia "Wywołanie statusu telefonu oraz tożsamości" oraz uprawnienia ustalenia lokalizacji.

Lista smartfonów kompatybilnych z systemem AirKey

Należy pamiętać, że kompatybilność smartfona zależy od wielu czynników i nie każdy smartfon spełniający wymagania minimalne będzie kompatybilny. Dlatego firma EVVA poddaje smartfony dokładnym testom. Stale aktualizowana lista modeli smartfonów przetestowanych i odpowiednich do użytku z systemem AirKey znajduje się na liście kompatybilnych smartfonów.

Uprawnienie **"Wywołanie statusu telefonu oraz tożsamości"** jest niezbędne do jednoznacznej identyfikacji smartfona podczas dodawania nowego systemu zamknięć.

Uprawnienie **ustalania lokalizacji jest potrzebne, ponieważ system Android 6+ wymaga aktywacji tej funkcji, aby możliwe było wyszukiwanie komponentów Bluetooth!** Jeśli użytkownik zamierza korzystać z funkcji Bluetooth w aplikacji AirKey, należy aktywować w ustawieniach urządzenia opcję ustalania lokalizacji oraz przydzielić aplikacji uprawnienie do tej funkcji. Jeśli użytkownik NIE zamierza aktywować funkcji ustalania lokalizacji, można utworzyć z komponentem (nośniki i komponent zamykające) połączenie NFC.

W przypadku **urządzeń Apple** (system operacyjny iOS) nie ma możliwości dezaktywacji uprawnienia "Wywołanie statusu telefonu oraz tożsamości". Ponadto system iOS może także wyszukiwać komponenty Bluetooth bez uprawnienia do ustalania lokalizacji.

3.4 Nośniki AirKey

Jako nośniki dostępu dostępne są sprawdzone modele smartfonowe oraz karty, przywieszki do kluczy, klucze Combi i bransoletki w różnych konfiguracjach jak np. w kombinacji z technologią *Mifare DESFire EV1*.

Odpowiednie arkusze specyfikacji oraz katalog produktów są dostępne na naszej stronie firmowej w sekcji materiałów do pobrania: https://www.evva.com/pl/downloads/.

Nośniki takie jak karty, breloki do kluczy, bransoletki i klucze Combi są dostarczane w stanie fabrycznym. Aby zastosować je w systemie AirKey, należy je najpierw dodać do systemu.

3.5 Moduł zarządzania online systemu AirKey

Moduł zarządzania online systemu AirKey to oprogramowanie online udostępnione przez firmę EVVA służące do administracji i zarządzania systemem AirKey. Elektroniczny system zamknięć AirKey działa w kombinacji ze wszystkimi popularnymi przeglądarkami internetowymi oraz systemami operacyjnymi i nie wymaga specjalnej infrastruktury IT. Zadania z zakresu bieżącego działania i konserwacji centrum obliczeniowego AirKey są realizowane przez firmę EVVA.

3.5.1 Wymagania systemowe

- Systemy operacyjne: Windows 10 (lub nowsza wersja), MacOS 10.15 (lub nowsza wersja), Linux
- Obecnie obsługiwane są następujące przeglądarki internetowe:
  Chrome, Firefox, Edge, Safari
- Aktywowana obsługa JavaScript w przeglądarce
- Podłączenie do Internetu (1 Mbit/s lub szybsze)
- Opcja dodatkowa: port USB 2.0 do obsługi stacji kodującej
- Port dostępu do Internetu 443 musi być dostępny.

Do rejestracji systemu zamknięć AirKey potrzebny jest ważny adres poczty e-mail.

3.6 Jednostki KeyCredit firmy EVVA

Do bieżącej eksploatacji systemu zamknięć niezbędne są jednostki KeyCredit, służące do przekazywania lub zmiany uprawnień dostępu. Jednostki KeyCredit dostępne są jako kredyt ilościowy (określona liczba możliwych zmian uprawnień dostępu bez ograniczenia czasowego) lub jako kredyt czasowy (nieograniczona liczba możliwych zmian uprawnień w określonym przedziale czasu). W zależności od wielkości i dynamiki użytkowania systemu AirKey operator może skorzystać z odpowiedniego pakietu jednostek KeyCredit, który można nabyć u wyspecjalizowanego dystrybutora produktów firmy EVVA. Szczegółowe informacje na temat dostępnych pakietów można znaleźć w katalogu produktów AirKey (https://www.evva.com/pl/downloads/).

3.7 Stacja kodująca

Za pomocą opcjonalnej stacji kodującej można aktualizować nośniki i komponenty zamykające AirKey lub dodawać je do systemu AirKey – podobnie jak za pomocą smartfona z uprawnieniem konserwacyjnym. Aplikacja przeznaczona do zainstalowania na stacji kodowania ma tę zaletę, że jest zgodna z aktualnymi przeglądarkami oraz, że stacja kodowania może być wykorzystana do aktualizowania komponentów zamykających i nośników także po wylogowaniu z Modułu zarządzania online systemu AirKey lub po zamknięciu przeglądarki.

Obsługiwane są następujące przeglądarki: Chrome, Firefox i Edge.

Wymagania systemowe:

- Port USB
- Java 7 lub nowsza wersja
- Sterownik stacji kodującej

Bliższe informacje na ten temat można znaleźć w rozdziale Instalacja stacji kodującej.

3.8 Zasilacz awaryjny

Na stronie czołowej wszystkich komponentów zamykających (poniżej logo firmy EVVA) znajduje się złącze. Dostęp do tego złącza można uzyskać, naciskając lekko do środka miejsce przy logo, po lewej stronie napisu (przy literze E) i odsuwając element z prawej strony (przy literze A). Wbudowane złącze służy wyłącznie do zasilania awaryjnego i nie jest używane w normalnej eksploatacji.

Zasilacz awaryjny zasila komponent zamykający – dzięki temu nadal możliwa jest obsługa komponentu w przypadku rozładowanej baterii. W tym celu należy podłączyć kabel połączeniowy zasilacza awaryjnego do odpowiedniego złącza i włączyć zasilacz. Dalsze działania na zasilaczu nie są konieczne. Do obsługi komponentu zamykającego AirKey potrzebny jest nośniki z ważnym uprawnieniem.

Należy pamiętać, że powinno być to uprawnienie stałe bez ograniczenia czasu ważności. Bliższe informacje na ten temat można znaleźć w rozdziale Nośniki awaryjne. Po otwarciu awaryjnym należy natychmiast wymienić baterie w komponencie zamykającym i zaktualizować komponent, aby ponownie umożliwić dostęp także za pomocą pozostałych nośników. Bliższe informacje na temat awaryjnego otwarcia można także znaleźć w rozdziale Wymiana baterii i otwarcie awaryjne.

Należy pamiętać, że czytnika naściennego AirKey nie można zasilać za pomocą zasilacza awaryjnego, ponieważ jest on zasilany zewnętrznie w połączeniu z centralką sterującą AirKey.

4 Uruchomienie

W tym rozdziale opisano początkowe czynności, które należy wykonać w celu uruchomienia systemu AirKey.

Na stronie internetowej https://www.evva.com/pl/airkey/website/ znajduje się materiał wideo przedstawiający początkowe czynności i procedurę uruchomienia systemu AirKey.

Jako wsparcie podczas montażu komponentów zamykających firma EVVA przygotowała następujący materiał:

- **Instrukcja montażu**:
  Firma EVVA przygotowała materiały pomocowe przydatne podczas montażu komponentów zamykających. Są one dostępne jako wersja neutralna językowo. Można je znaleźć w opakowaniu danego produktu lub pobrać ze strony https://www.evva.com/pl/downloads/.
- **Materiały** wideo:
  Na stronie internetowej https://www.evva.com/pl/airkey/website/ udostępniono odpowiednie filmy wideo na temat montażu.

4.1 Instalacja aplikacji AirKey

- Wczytać aplikację AirKey z witryny Google Play Store lub Apple App Store.
- Postępować zgodnie z instrukcjami wyświetlanymi podczas instalacji aplikacji AirKey na smartfonie.

4.2 Rejestracja w Module zarządzania online systemu AirKey

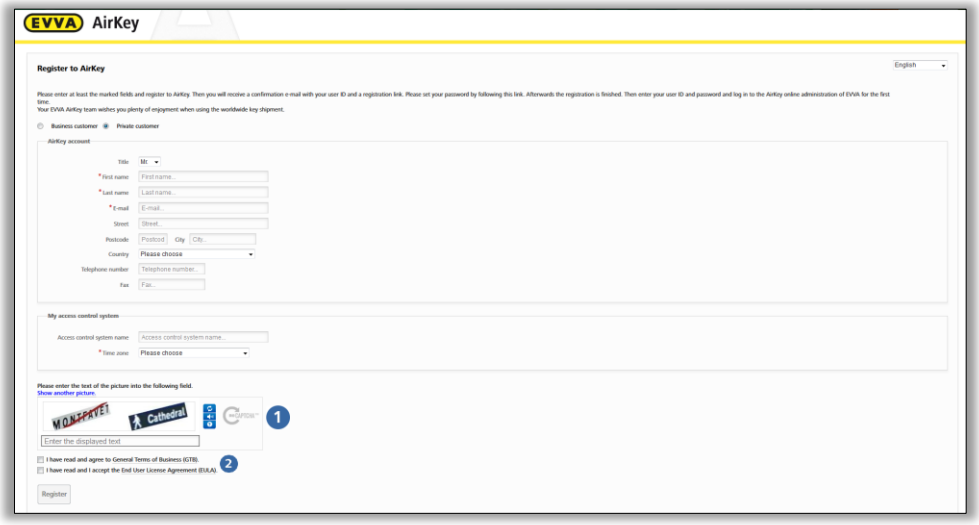
Aby korzystać z modułu zarządzania online, należy zarejestrować się w firmie EVVA, podając ważny adres poczty e-mail.

- Otworzyć w przeglądarce internetowej stronę https://airkey.evva.com.
  Otworzy się strona logowania do Modułu zarządzania online systemu AirKey.
- Wybrać preferowany język za pomocą opcji ***Język***.
- Kliknąć link ***Rejestracja w systemie AirKey*** ❶.

Rys. 3: Link "Rejestracja w systemie AirKey"

W oknie logowania należy wypełnić pola i zgłosić rejestrację systemu AirKey.

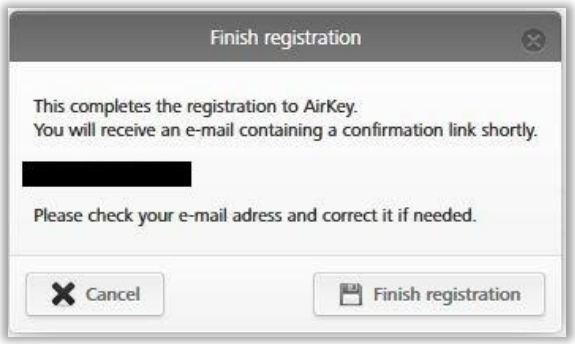
- Wybrać opcję ***Klient firmy*** lub ***Klient prywatny***.
- Wypełnić pola formularza.
  Pola oznaczone gwiazdką (*) są obowiązkowe.
- Rozwiąż zadanie Captcha ❶.
- Aktywować pole wyboru z linkiem Ogólne Warunki Handlowe (EVVA-OWH) oraz pole wyboru z linkiem Ogólne Warunki Licencyjne (EVVA-OWL) ❷. Automatycznie otworzą się dwa odpowiednie dokumenty PDF. Te dokumenty można wywołać także pod adresem https://www.evva.com/pl/airkey/impressum/.



Rys. 4: Rejestracja w systemie AirKey

W razie potrzeby dane klienta można zawsze zmienić w dowolnym momencie. W tym celu należy w menu głównym modułu zarządzania online kliknąć opcje ***System zamknięć*** → ***Dane klienta***.

- Kliknąć przycisk ***Zarejestruj***. Otworzy się okno użytkownika "Zakończ rejestrację".
- Sprawdzić jeszcze raz podany adres poczty e-mail, na który zostanie wysłane potwierdzenie z linkiem rejestracyjnym.
- Jeśli wyświetlony adres e-mail jest nieprawidłowy, należy przerwać operację za pomocą przycisku ***Anuluj*** i poprawić wprowadzone dane.
- Jeśli adres e-mail jest prawidłowy, należy zakończyć operację, klikając przycisk ***Zakończ rejestrację***.

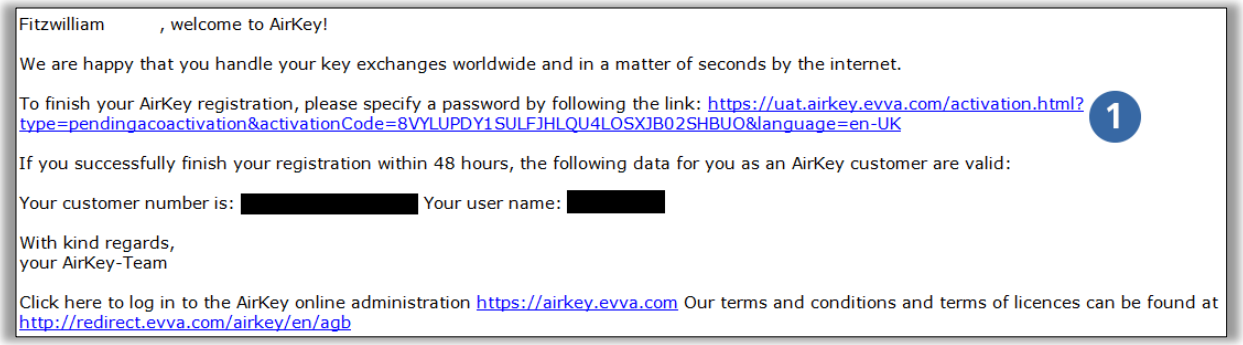


Rys. 5: Zakończenie rejestracji

System AirKey automatycznie wygeneruje identyfikator i link rejestracyjny i prześle te informacje jako wiadomość rejestracyjną na podany adres poczty e-mail.

- Otworzyć konto poczty e-mail. W skrzynce będzie wiadomość od firmy EVVA w sprawie systemu AirKey, o temacie: "Rejestracja w systemie EVVA AirKey".
- Otworzyć wiadomość e-mail i kliknąć link rejestracyjny ❶.

Otrzymaną wiadomość e-mail należy zachować. Zawarte w nim jednoznaczny identyfikator i numer klienta będą potrzebne w razie potrzeby uzyskania wsparcia.


Fitzwilliam , welcome to AirKey!

We are happy that you handle your key exchanges worldwide and in a matter of seconds by the internet.

To finish your AirKey registration, please specify a password by following the link: https://uat.airkey.evva.com/activation.html?type=pendingacoactivation&activationCode=8VYLUPDY1SULFJHLQU4LOSXJB02SHBUO&language=en-UK 1

If you successfully finish your registration within 48 hours, the following data for you as an AirKey customer are valid:

Your customer number is: [redacted] Your user name: [redacted]

With kind regards,
your AirKey-Team

Click here to log in to the AirKey online administration https://airkey.evva.com Our terms and conditions and terms of licences can be found at http://redirect.evva.com/airkey/en/agb

Rys. 6: Wiadomość e-mail dotyczący rejestracji systemu AirKey firmy EVVA

Link rejestracyjny jest ważny tylko przez 48 godzin.

Jeśli ważność linku rejestracyjnego upłynie lub adres strony rejestracyjnej będzie nieprawidłowy, pojawi się komunikat błędu "Nieprawidłowy link do rejestracji". W takim przypadku należy zarejestrować się ponownie.

Po kliknięciu linku do rejestracji otworzy się okno powitalne, służące do zakończenia procesu rejestracji.

- Wprowadzić wybrane hasło dla Modułu zarządzania online systemu AirKey. Hasło systemu AirKey musi składać się z co najmniej 6 znaków, jednej cyfry, jednej wielkiej i jednej małej litery – w przeciwnym razie pojawi się komunikat błędu.
- Ponownie wprowadzić hasło.

> Wprowadzić swoją datę urodzenia. Będzie ona wykorzystana jako pytanie bezpieczeństwa w przypadku utraty hasła.

Z przyczyn związanych z bezpieczeństwem zalecamy stosowanie możliwie długiego hasła systemu AirKey i zachowanie go w tajemnicy.

Rys. 7: Definiowanie własnego hasła systemu AirKey w celu zakończenia rejestracji

> Jeśli pola obowiązkowe zostały wypełnione i obydwa wprowadzone hasła systemu AirKey są identyczne, należy zakończyć rejestrację, klikając przycisk ***Zapisz*** ❶.

W tym momencie proces rejestracji został zakończony i system zamknięć AirKey został aktywowany.

Od teraz można logować się w oknie logowania Modułu zarządzania online systemu AirKey. Do tego celu potrzebny jest identyfikator z rejestracyjnej wiadomości e-mail oraz zdefiniowane hasło systemu AirKey.

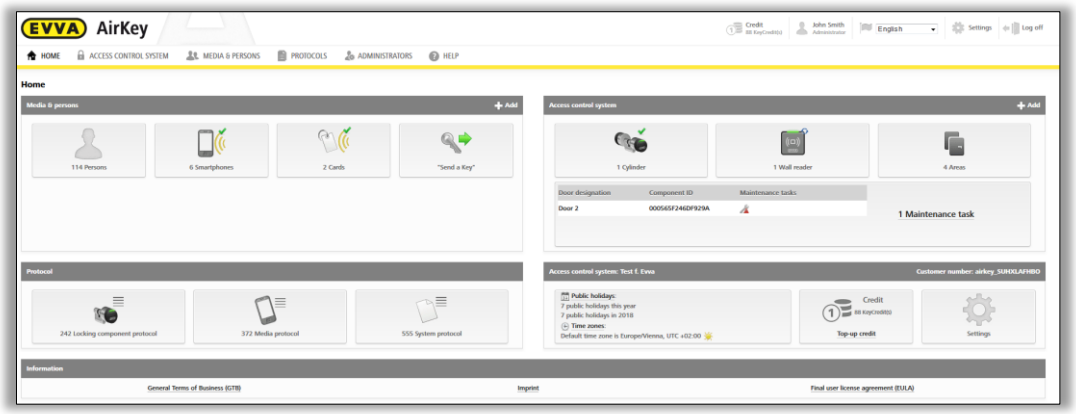
4.3 Logowanie

Logowanie jest konieczne, aby wykonać konfigurację lub czynności administracyjne w systemie AirKey.

> Otworzyć w przeglądarce internetowej stronę https://airkey.evva.com.
Otworzy się strona logowania do Modułu zarządzania online systemu AirKey.

> Wybrać preferowany język za pomocą opcji ***Język***. W ramach aktywnej sesji można w dowolnym momencie zmienić ustawienia języka na pasku menu z prawej strony.

> Wprowadzić identyfikator podany w rejestracyjnej wiadomości e-mail i zdefiniowane hasło, a następnie potwierdzić przyciskiem ***Zaloguj się***. Otworzy się strona startowa systemu AirKey.

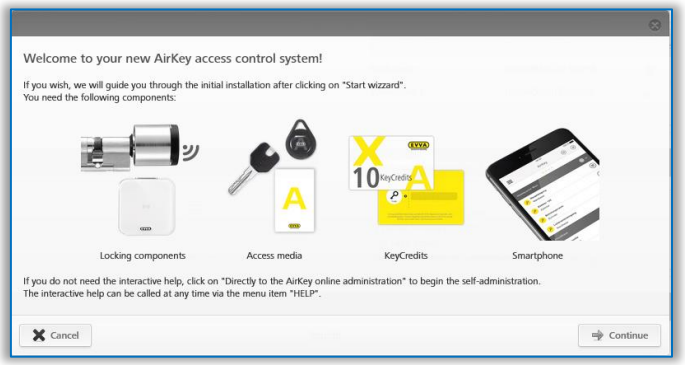


Rys. 8: Strona startowa systemu AirKey

Na stronie startowej wyświetlono przegląd wszystkich ważnych danych dotyczących danego systemu. Z tego miejsca można przejść do wszystkich funkcji i ustawień.

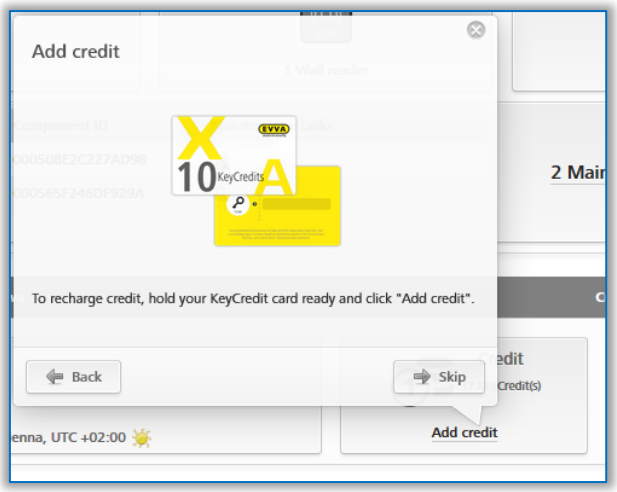
4.4 Interaktywna pomoc

W Module zarządzania online systemu AirKey, po pierwszym zalogowaniu uruchomi się interaktywna pomoc, która przedstawi i wyjaśni najważniejsze funkcje programu.



Rys. 9: Interaktywna pomoc

Jako przykład pokazano funkcję "Doładowanie środków". Interaktywna pomoc wskaże, które przyciski należy kliknąć, oraz wyświetla wskazówki o tym, jakie informacje należy wprowadzić. W ramach pomocy interaktywnej można nawigować, przełączając strony do przodu lub wstecz.



Rys. 10: interaktywna pomoc – doładowanie środków

Można także zamknąć interaktywną pomoc i poznać Moduł zarządzania online systemu AirKey, korzystając z podręcznika systemu.

Jeśli interaktywna pomoc została zamknięta i użytkownik chciałby ją ponownie wywołać, należy w menu głównym wybrać opcje ***Pomoc*** → ***Interaktywna pomoc***. W ten sposób można w dowolnym momencie skorzystać z interaktywnej pomocy.

4.5 Instalacja stacji kodującej

Option Opcjonalna stacja kodująca AirKey służy do aktualizowania lub dodawania komponentów zamykających i nośników do systemu AirKey.

Aby korzystać ze stacji kodującej w systemie AirKey, należy zainstalować aplikację stacji kodującej.

Istnieją dwie możliwości użycia stacji kodującej:

- w przeglądarce, poprzez Moduł zarządzania online systemu AirKey
- bez przeglądarki, poprzez wiersz poleceń

4.5.1 Używanie stacji kodującej poprzez Moduł zarządzania online systemu AirKey

Aplikacja przeznaczona do zainstalowania na stacji kodowania ma tę zaletę, że jest zgodna z aktualnymi przeglądarkami oraz, że stacja kodowania może być wykorzystana do aktualizowania komponentów zamykających i nośników także po wylogowaniu z Modułu zarządzania online systemu AirKey lub po zamknięciu przeglądarki.

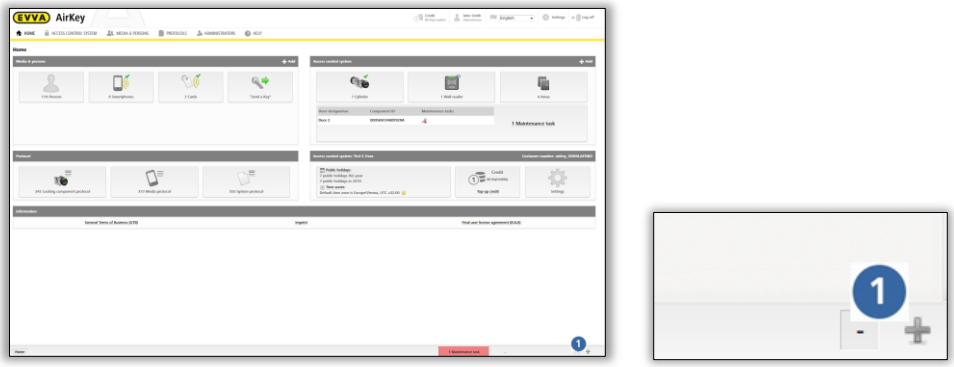
Dodawanie i usuwanie komponentów zamykających do systemu zamknięć oraz aktualizacja oprogramowania firmware komponentów zamykających lub aktualizacja Keyring z nośników dostępu jest możliwa tylko po zalogowaniu w Module zarządzania online systemu AirKey. Aktualizacje nośników i komponentów zamykających są możliwe także po wylogowaniu z Modułu zarządzania online systemu AirKey lub po zamknięciu przeglądarki.

Poniższe przeglądarki obsługują komunikację między Modułu zarządzania online systemu AirKey a lokalną aplikacją stacji kodującej: Chrome, Firefox i Edge.

Sposób pobierania i obsługa aplikacji stacji kodującej zależy od przeglądarki i systemu operacyjnego. Widok w przeglądarce może się różnić od zaprezentowanego tutaj widoku (Firefox).

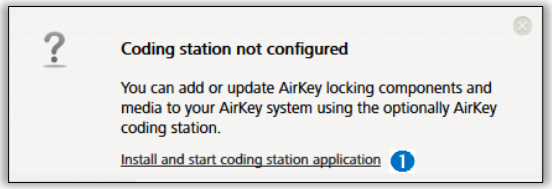
Zarejestrować i zalogować się w Module zarządzania online systemu AirKey (patrz rozdział Rejestracja w Module zarządzania online systemu AirKey).

- Podłączyć stację kodującą do złącza USB w komputerze.
- W Module zarządzania online systemu AirKey kliknąć symbol **+** w prawej dolnej części ekranu ❶.



Rys. 11: Stacja kodująca – instalacja stacji kodującej

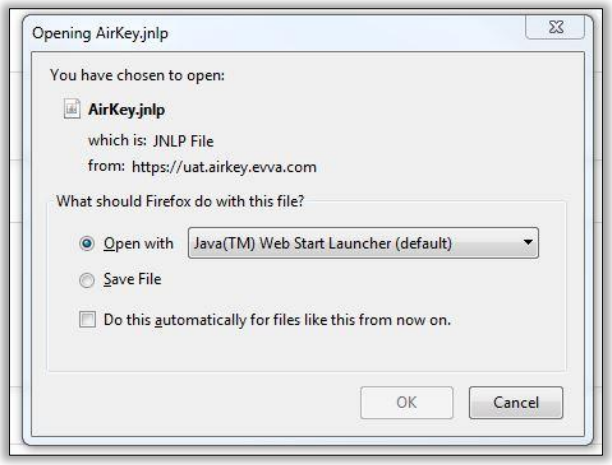
- Aby zainstalować aplikację stacji kodującej, należy kliknąć link "Instalowanie i uruchomienie aplikację stacji kodującej" ❶.



Rys. 12: Instalowanie i uruchomienie aplikację stacji kodującej

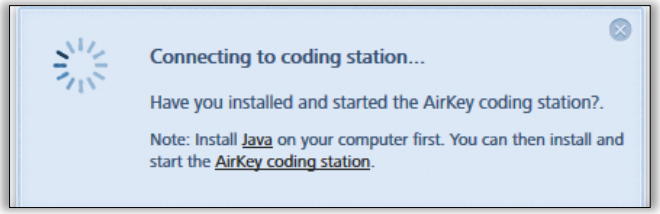
Po kliknięciu linku użytkownik będzie miał 60 sekund czasu na otworzenie pliku AirKey.jnlp (patrz kolejny krok). W razie przekroczenia czasu należy powtórzyć bieżący krok procedury. Alternatywnie można również zapisać plik AirKey.jnlp i otworzyć ręcznie.

- Pojawi się okno dialogowe pobierania pliku AirKey.jnlp. Otworzyć plik za pomocą aplikacji "Java(TM) Web Start Launcher".



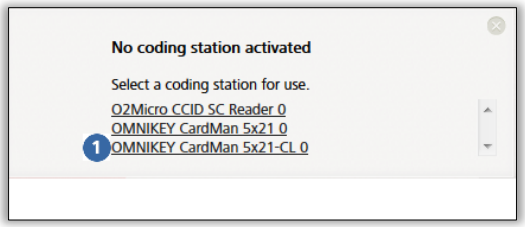
Rys. 13: Otwieranie pliku AirKey.jnlp

> Po uruchomieniu pliku zostanie nawiązane połączenie ze stacją kodującą.



Rys. 14: Utworzenie połączenia ze stacją kodującą

> Wybrać istniejącą stację kodującą (np. "OMNIKEY CardMan 5x21-CL 0" ❶) z listy.



Rys. 15: Wybór stacji kodującej

> Na pasku zadań w prawym dolnym rogu pojawi się ikona AirKey – stacja kodująca została prawidłowo zainstalowana i jest aktywna.

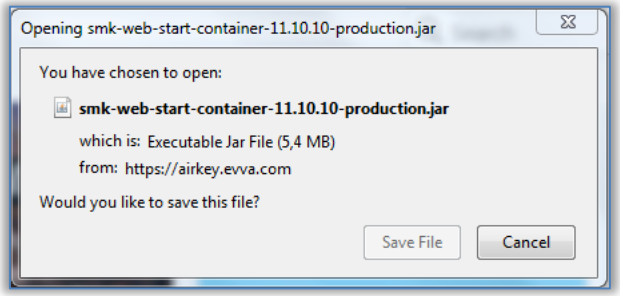
Rys. 16: Ikona AirKey na pasku zadań

4.5.2 Używanie stacji kodującej poprzez wiersz poleceń

Aplikacja stacji kodowania może być zainstalowana i skonfigurowana także bez modułu zarządzania online AirKey, np. z wiersza poleceń. (Opcja ta wymaga zaawansowanej wiedzy w zakresie IT, zwłaszcza w zakresie korzystania z wiersza poleceń.)

Poprzez wiersz poleceń stacja kodująca może być używana tylko do aktualizacji nośników dostępu i komponentów zamykających. Aktualizacja firmware komponentów zamykających jest możliwa tylko za pomocą przeglądarki lub smartfonu z uprawnieniem do konserwacji.

> Zapisz aplikację stacji kodowania korzystając z łącza https://airkey.evva.com/smkrest/jnlp/newest-jar-file/ w dowolnym katalogu.



Rys. 17: Pobierz aplikację stacji kodowania

> Otwórz wiersz poleceń i nawiguj do katalogu, w którym została wcześniej zapisana aplikacja stacji kodowania.

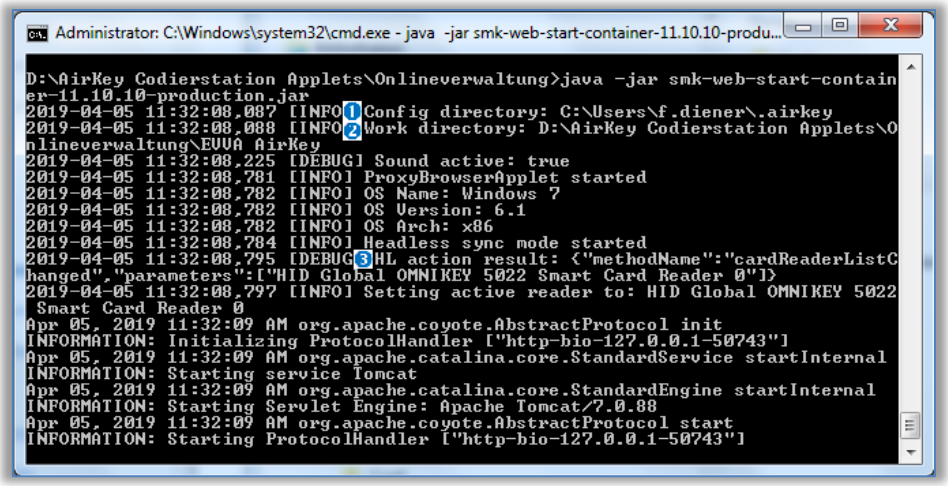
> Uruchom aplikację stacji kodowania za pomocą następującego polecenia:

`java -jar <nazwa pliku>`
(np. `web-start-container-customer-15.10.0-8.jar`)

Dodatkowo można wprowadzić następujące parametry opcjonalne:

- **`-reader "<nazwa stacji kodującej>"`**: Za pomocą tego parametru można zastosować określoną stację kodującą. (np. "HID Global OMNIKEY 5022 Smart Card Reader 0"). W takim przypadku plik konfiguracyjny `config_customer.json` zostanie zignorowany.
- **`-port <WARTOŚĆ [1024-65535]>`**: Jeśli ten parametr nie jest określony, domyślnie używany jest port 50743. Port 50743 jest także używany, gdy stacja kodująca jest używana przez Moduł zarządzania online systemu AirKey w przeglądarce internetowej. Jeśli użytkownik chce korzystać z kilku stacji kodującej równolegle na jednym komputerze, dla każdej stacji kodującej musi podać osobny port. Parametr "**`-port 0`**" używa portu losowego.
- **`-configDir <WARTOŚĆ>`**:W podanym folderze (domyślnie dla Windows: `%USERPROFILE%\.airkey`) zapisywany jest plik konfiguracyjny `config_customer.json`. Zostanie ona automatycznie wygenerowana przy pierwszym uruchomieniu aplikacji stacji kodującej i zapisze ostatnio używane ustawienia.
- **`-workDir <WARTOŚĆ>`**:W podanym folderze tworzony jest np. plik dziennika `logs\application.log` po uruchomieniu aplikacji stacji kodowania. Zostaną w nim zaprotokołowane wszystkie czynności, które zostały wykonane za pomocą aplikacji stacji kodującej. W przypadku równoległego używania kilku stacji kodującej zaleca się użycie dla każdej stacji kodującej osobnego folderu.
- **`-version`**: Wyświetla wersję aplikacji stacji kodowania.
- **`-help`**: Otwiera Pomoc zawierającą opis wszystkich dostępnych parametrów.

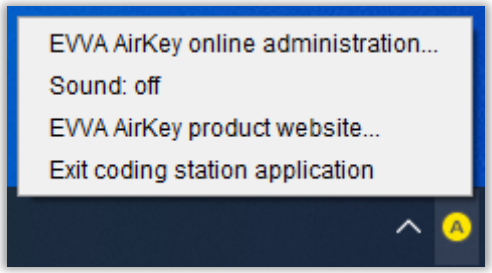
- Na liście zadań w prawym dolnym rogu ukaże się ikona AirKey a w wierszu poleceń zostaną wyświetlone informacje o katalogu konfiguracji ❶, katalogu roboczym ❷ i dostępnych stacjach kodowania ❸.



Rys. 18: Start aplikacji stacji kodowania z wiersza poleceń

4.5.3 Ustawienia aplikacji stacji kodującej

Po kliknięciu ikony AirKey prawym przyciskiem myszy otworzy sich odpowiednie menu kontekstowe.



Rys. 19: Ustawienia aplikacji stacji kodującej

Lista odpowiednich punktów menu:

- ***Moduł zarządzania online systemu EVVA AirKey...*** – link do strony logowania Modułu zarządzania online systemu AirKey
- ***Dźwięk: wł.*** – zostanie wygenerowany sygnał dźwiękowy po aktualizacji komponentu za pomocą stacji kodującej. Ta funkcja jest przydatna jako informacja zwrotna, gdy stacja kodująca jest użytkowana bez Modułu zarządzania online systemu AirKey. Po kliknięciu ***Dźwięk: wł.*** następuje przełączenie na ***Dźwięk: wył.***
- ***Dźwięk: wył.*** – nie będzie wyprowadzany sygnał dźwiękowy. Po kliknięciu ***Dźwięk: wył.*** nastąpi przełączenie na ***Dźwięk: wł.***
- ***Strona internetowa produktu EVVA AirKey...*** – link do strony internetowej produktu AirKey
- ***Zakończ aplikację stacji kodującej*** – zamknięcie aplikacji stacji kodującej.

4.5.4 Rozwiązywanie możliwych problemów ze stacją kodującą

Po podłączeniu stacji kodującej dioda świecąca sygnalizuje gotowość do pracy. W razie braku sygnalizacji gotowości do pracy należy odłączyć stację kodującą i ponownie ją podłączyć. Ewentualnie należy ponownie zainstalować sterownik stacji kodującej.

Przy wyłączaniu komputera nastąpi automatyczne zamknięcie lokalnej aplikacji stacji kodującej. Aby uruchomić automatycznie aplikację podczas ponownego uruchomienia komputera, można za pomocą panelu sterowania Java™ (konfiguracja Java) utworzyć skrót aplikacji (aplikacja: AirKey Card Reader Proxy; typ: aplikacja) i przenieść go do folderu Autostart.

Aplikacja stacji kodującej zamyka się po uruchomieniu

Aplikacja stacji kodującej wykorzystuje standardowo port 50743 do komunikacji z przeglądarką. Jeśli port jest używany przez inny program, nie można uruchomić aplikacji stacji kodowania. W systemie Windows 10 lub nowszym można używać tego portu Hyper-V. Aby zapobiec użyciu tego portu przez Hyper-V, można:

- Wyłączyć Hyper-V:
  ```
  C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V
  ```
- Uruchom ponownie komputer.
- Dodaj wyjątek dla portu 50743:
  ```
  C:\> netsh int ipv4 add excludedportrange protocol=tcp startport=50743
       numberofports=1
  ```
- Reaktywacja Hyper-V:
  ```
  C:\> dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All
  ```
- Uruchom ponownie komputer.

Jako stację kodującą wybrano czytnik kart "Microsoft UICC"

Rys. 20: Czytnik kart "Microsoft UICC" w Module zarządzania online systemu AirKey

W ramach rozwiązania można wyłączyć czytnik kart UICC w menedżerze urządzeń Windows: Menadżer urządzeń → Urządzenia programowe → Microsoft UICC ISO Reader → Wyłącz urządzenie

Połączenie ze stacją kodującą nie może zostać nawiązane przez Moduł zarządzania online systemu AirKey (https proxy)

Zarówno Moduł zarządzania online systemu AirKey, jak i aplikacja stacji kodującej komunikują się z systemem AirKey za pomocą zaszyfrowanego portu 443. W sieciach korzystających z serwera proxy https może być jednak konieczne zdefiniowanie wyjątku dla

"airkey.evva.com" i poddomen, ponieważ aplikacja stacji kodującej sprawdza certyfikat serwera za pomocą "certificate pinning", a tym samym nie dopuszcza żadnych proxys https.

Połączenie ze stacją kodującą nie może zostać nawiązane przez Moduł zarządzania online systemu AirKey (ochrona przed rebinowaniem DNS)

Moduł zarządzania online systemu AirKey komunikuje się lokalnie między przeglądarką a aplikacją stacji kodującej. Czynności, takie jak nakładanie komponentów zamykających lub nośników dostępowych na stację kodującą, są wyświetlane w Module zarządzania online systemu AirKey.

Przeglądarka łączy się z aplikacją stacji kodującej poprzez "components.airkey.evva.com" (port 50743). Ten adres URL jest usuwany przez serwer DNS jako 127.0.0.1.

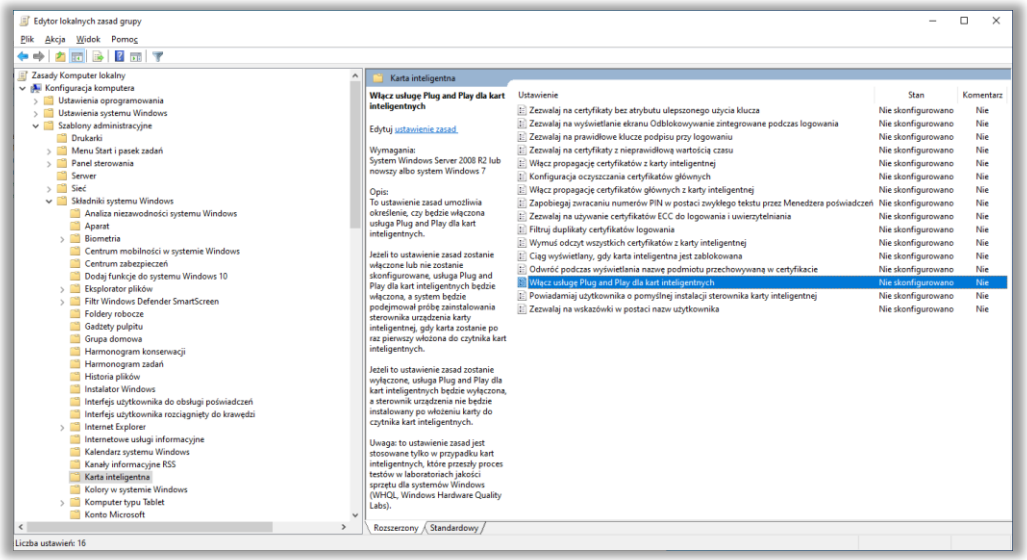
Dlatego przy aktywnej ochronie *DNS-rebinding* może być konieczne dodanie wyjątków dla "components.airkey.evva.com" i poddomen z "airkey.evva.com".

Windows wielokrotnie szuka sterownika stacji kodującej

Podczas nakładania komponentu zamykającego lub nośnika dostępowego na stację kodującą system Windows próbuje wyszukać i zainstalować sterownik stacji kodującej. Może to mieć wpływ na komunikację ze stacją kodującą i prowadzić do nieprawidłowego działania.

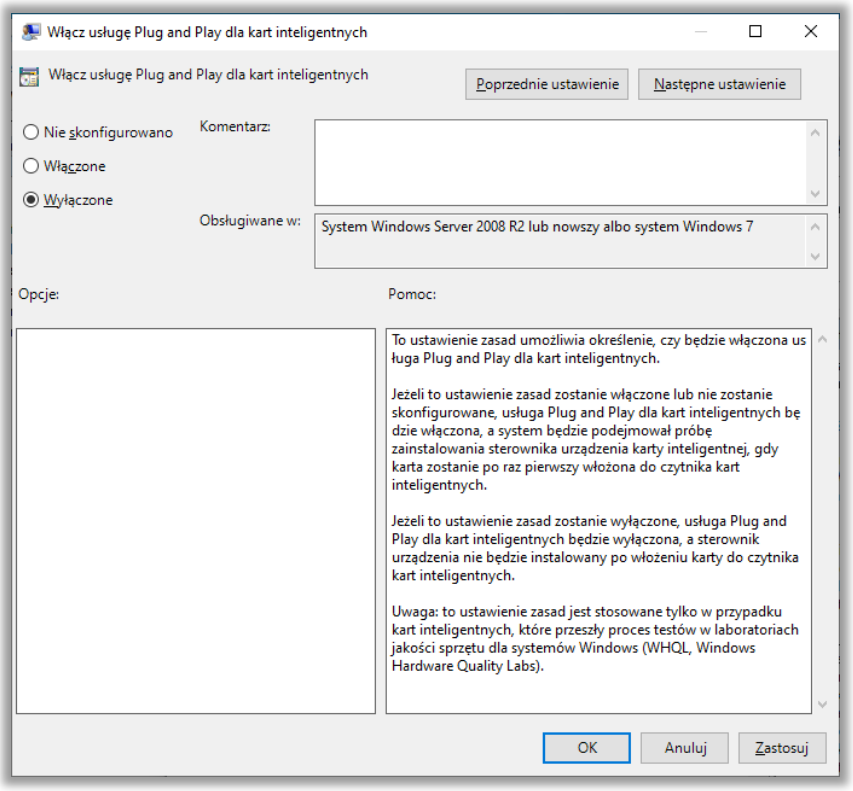
W ramach rozwiązania można dezaktywować usługę Smart Card Plug & Play systemu Windows:

- Przycisk Windows + R
- Wprowadzić "gpedit.msc" i potwierdzić przyciskiem ***Enter***.
- Program "Edytor lokalnych zasad grupy" ⟶ Konfiguracja komputera ⟶ Szablony administracyjne ⟶ Składniki systemu Windows ⟶ Karta inteligentna
- Kliknąć dwukrotnie wiersz z wpisem "Usługa Plug and Play dla kart inteligentnych" po prawej stronie.



Rys. 21: Edytor lokalnych zasad grupy

- Wybrać przycisk opcji ***Wyłączone***.
- Potwierdź przyciskiem ***OK***.



Rys. 22: Usługa Plug and Play dla kart inteligentnych

W systemie MacOS 11.x lub nowszym nie można wybrać stacji kodującej

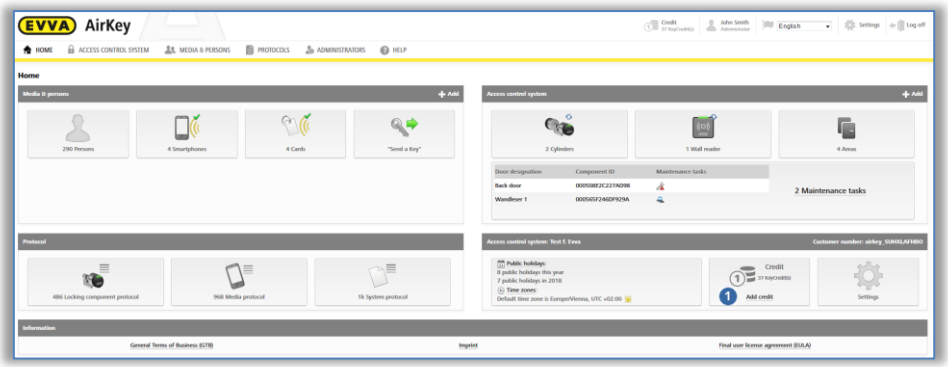
Od MacOS Big Sur (11.x) w systemie Mac nie jest już możliwe wybieranie podłączonej stacji kodującej za pośrednictwem Modułu zarządzania online systemu AirKey. Aplikację stacji kodującej można wprawdzie uruchomić pomyślnie, ale w Module zarządzania online systemu AirKey nie będzie wyświetlana żadna stacja kodująca.

W ramach rozwiązania stację kodującą można uruchomić za pomocą wiersza poleceń (patrz rozdział Używanie stacji kodującej poprzez wiersz poleceń). Warunkiem jest jednak zainstalowanie wersji Java JDK17 (Oracle JDK17 lub OpenJDK17) lub nowszej.

4.6 Doładowanie środków

Potrzebna będzie do tego karta KeyCredit. Na jej tylnej stronie, na zakrytym polu (do zdrapania) znajduje się kod kredytu.

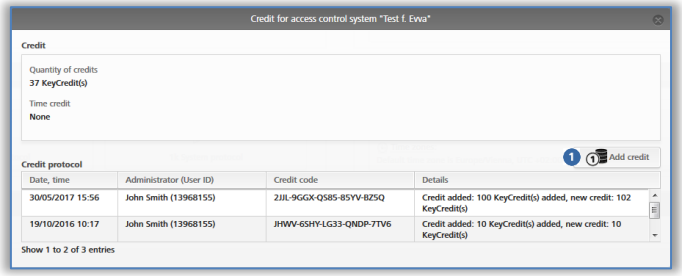
- Na stronie startowej ***Home*** wybrać ikonę ***Dodaj kredyt*** ❶.
- Alternatywnie można kliknąć opcję ***Kredyt*** w wierszu nagłówka.



Rys. 23: Kredyt

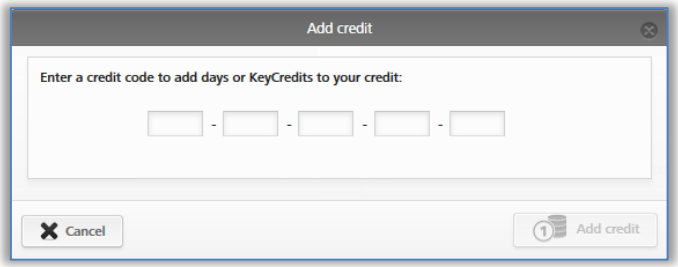
> Zostanie wyświetlony przegląd aktualnego kredytu i już uruchomione doładowania.

> Kliknąć przycisk ***Dodaj kredyt*** ❶.



Rys. 24: Doładowanie środków

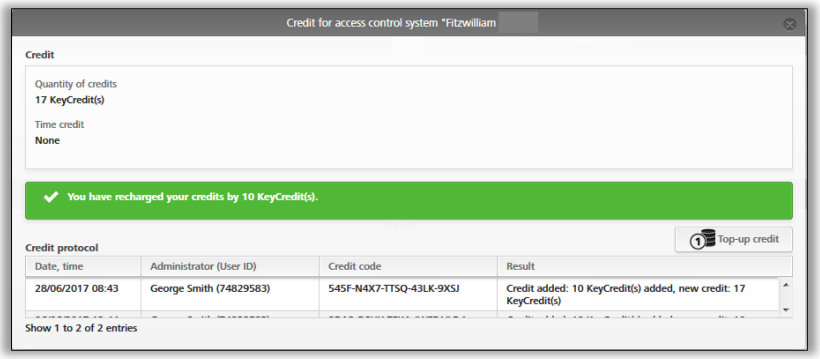
> W oknie doładowania środków wprowadzić kod, który znajduje się na zakrytym polu karty KeyCredit.



Rys. 25: Wprowadzenie kodu doładowania środków

> Kliknąć opcję ***Dodaj kredyt***.

Jeśli wprowadzono poprawny kod, wpisana wartość zostanie potwierdzona a środki zostaną zaksięgowane.

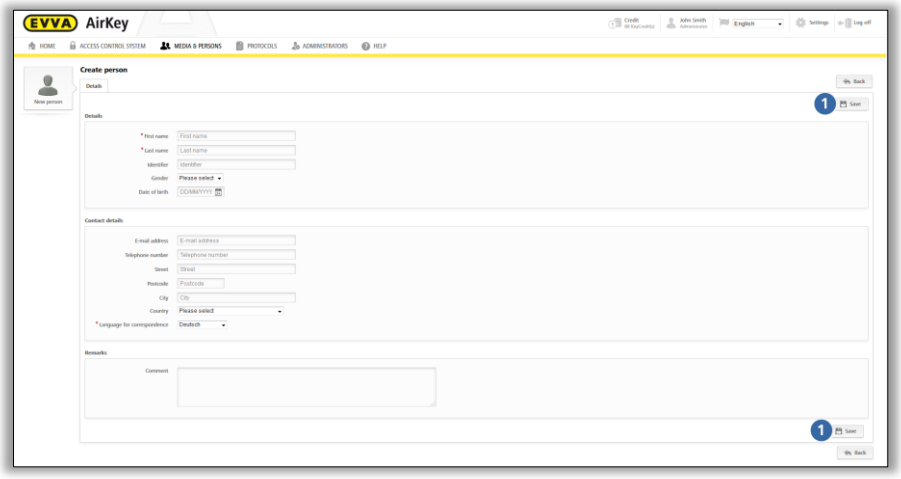


Rys. 26: Doładowanie środków

4.7 Utworzenie osoby

Każda osoba, która otrzyma uprawnienie w ramach systemu zamknięć AirKey, musi zostać najpierw utworzona w systemie.

- Na stronie startowej ***Home*** na szarym pasku bloku ***Nośniki i osoby*** kliknąć opcje ***Dodaj*** → ***Utwórz osobę***.
- Alternatywnie można wybrać na stronie startowej ***Home*** ikonę ***Osoby*** → ***Utwórz osobę***.
- Alternatywnie w menu głównym można wybrać opcje ***Nośniki i osoby*** → ***Utwórz osobę***.
- Alternatywnie można wybrać przycisk ***"Send a Key"***oraz kliknąć opcję ***Utwórz nowy***. Tutaj można utworzyć osobę ze smartfonem.
- Wypełnić pola formularza. Pola oznaczone gwiazdką (*) są obowiązkowe.
- Kliknąć przycisk ***Zapisz*** ❶.



Rys. 27: Utworzenie osoby

Pola "Imię" / "Nazwisko" / "Identyfikator" stanowią jednoznaczną kombinację w ramach systemu zamknięć AirKey.

W razie dodatkowego wypełnienia pola "Identyfikator" należy zastosować wartość, która zagwarantuje, że kombinacja z imieniem i nazwiskiem będzie

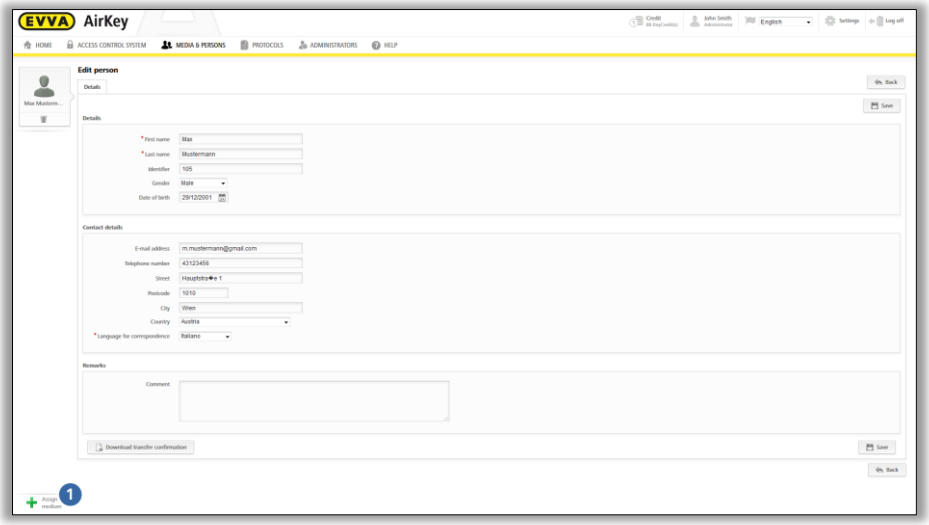
jednoznaczna (np. numer pracownika). Ma to znaczenie zwłaszcza wówczas, gdy określone osoby mają takie same imiona i nazwiska.

Długość wprowadzanych wartości dla każdego z pól "Adres e-mail", "Numer telefonu", "Ulica", "Kod pocztowy" i "Miejscowość" jest ograniczona do 50 znaków. W polu kodu pocztowego można użyć maksymalnie 10 znaków. W polu "Komentarz" można wprowadzić tekst o maksymalnej długości 500 znaków.

Jeśli wprowadzona kombinacja została już utworzona, pojawi się komunikat błędu "Ta osoba już istnieje".

- Sprawdzić i ew. poprawić wprowadzone dane.
- Kliknąć przycisk ***Zapisz***.

Jeśli utworzenie osoby w systemie powiodło się, pojawi się odpowiedni komunikat i pod nazwiskiem pojawi się nowy przycisk ***Przypisz nośnik*** ❶.

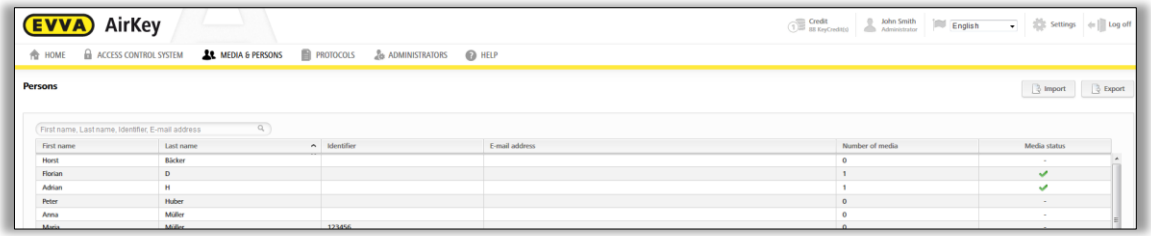


Rys. 28: Przyporządkowanie nośnika

W ten sposób osoba została utworzona w systemie zamknięć AirKey i zostanie uwzględniona na liście osób.

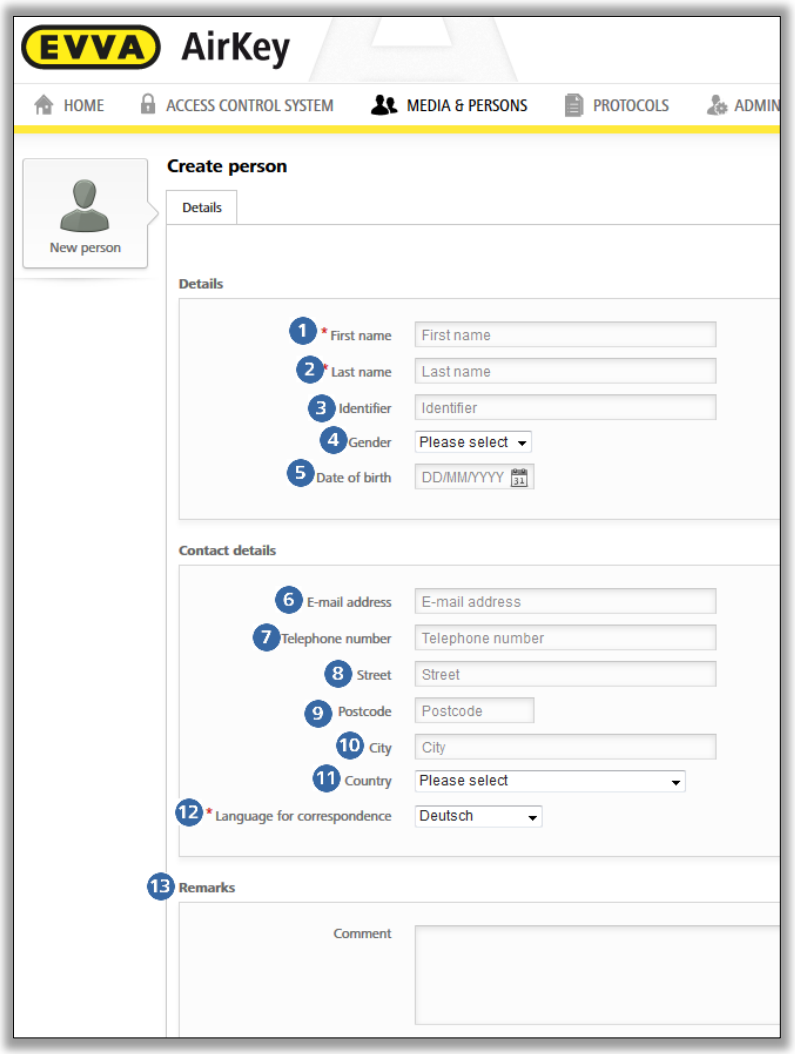
4.7.1 Import danych osobowych

W systemie AirKey istnieje możliwość utworzenia osób za pomocą zewnętrznych plików. Do tego celu potrzebny będzie plik CSV, który posłuży do zaimportowania tych danych do Modułu zarządzania online systemu AirKey ❶.

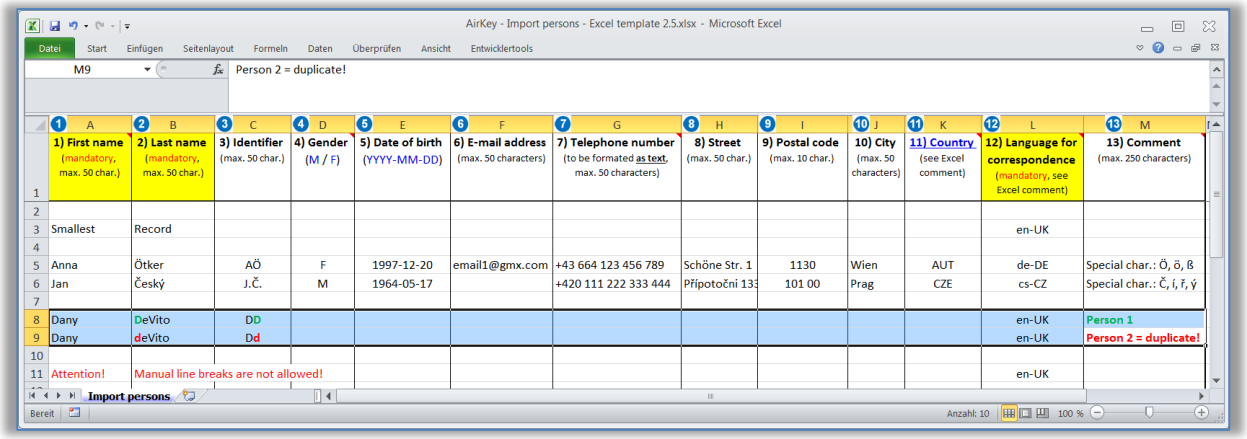


Rys. 29: Import listy osób

Podział tabeli osób odzwierciedla arkusz w oknie ***Utwórz osobę*** w Module zarządzania online systemu AirKey, tzn. kolumna A to imię ❶, kolumna B to nazwisko ❷, kolumna C to identyfikator ❸ itp. Dokładnie w tej kolejności odbywa się import pliku CSV do Modułu zarządzania online systemu AirKey.



Rys. 30: Import osób – lista osób



Rys. 31: Import osób – podział pól na liście osób

Właściwości pliku CSV z importowanymi danymi osobowymi:

- Pierwszy wiersz jest zawsze ignorowany. Dlatego zaleca się, aby umieścić w nim nazwy pól, aby łatwiej zidentyfikować kolejne dane. Pierwszy wiersz może także pozostać pusty, ale nie powinien zawierać danych żadnej osoby, ponieważ nie zostaną one zaimportowane.
- Pusty wiersz lub wiersze, które zawierają tylko spacje lub tabulacje (czyli puste pola), zostaną zignorowane. Jeśli użytkownik chciałby przejrzyściej zorganizować swoje pliki CSV, można stosować dowolną liczbę pustych wierszy.
- Każdy wiersz musi zawierać wszystkie 13 pól (atrybutów), które przedstawiono na Rys. 30.
- Pola są rozdzielone średnikiem.
- Istnieją tylko 3 pola obowiązkowe: imię (pole 1), nazwisko (pole 2) oraz język do korespondencji (pole 12).
- Jeśli pozostałe pola nie zawierają danych, muszą być uwzględnione mimo braku treści jako pola puste (;;).
- Płeć (pole 4) może zawierać wyłącznie wartości **M** (*male* = mężczyzna) lub **F** (*female* = kobieta) lub być pusta. Wartości M i F obowiązują dla wszystkich języków – należy stosować duże litery.
- Data urodzin (pole 5) musi mieć format **RRRR-MM-DD** (np. 1997-12-20).
- Adres e-mail (pole 6) musi zawierać znak **@** wraz z pozostałymi znakami lub być pusta.
- Kraj dla adresu (pole 10) musi zawierać 3-znakowy kod ISO 3166-1 (kolumna alfa-3) kraju lub być pusty. Kod musi składać się wyłącznie z dużych liter. Przykłady: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL itd.
- Język korespondencji (pole 12) jest polem obowiązkowym i musi zawierać kod ISO danego języka. Pisownia musi zawierać małe i duże – należy jej ściśle przestrzegać. Akceptowane są wyłącznie następujące kody: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- Importowana osoba będzie wskazywana jako już istniejąca (symbol ⚠), jeśli będzie już dostępna kombinacja imię + nazwisko + identyfikator (pola 1-3) w Module zarządzania online systemu AirKey, także wówczas, gdy pozostałe pola (4-13) będą mieć inną wartość. Takie osoby nie zostaną zaimportowane. W pisowni nazw nie uwzględnia się użycia dużych/małych liter (np. nazwy "Danny;**D**eVito;D**D**" i "Danny;**d**eVito;D**d**" będą traktowane jako ta sama osoba i tylko pierwsza osoba zostanie zaimportowana).
- Osoba będzie interpretowana jako duplikat w pliku CSV, gdy kombinacja imię + nazwisko + identyfikator (pola 1-3) została już raz znaleziona, także wówczas, gdy pozostałe pola (4-13) będą mieć inną wartość. W takim przypadku zostanie wyświetlony i zaimportowany tylko pierwszy wiersz z określoną kombinacją. Wszystkie pozostałe duplikaty zostaną zignorowane i nie będą wyświetlone w tabeli osób do zaimportowania.
- Plik CSV nie może przekraczać danych maksymalnych. Jeśli chcesz zaimportować więcej osób, utwórz wiele plików CSV, które możesz zaimportować osobno.

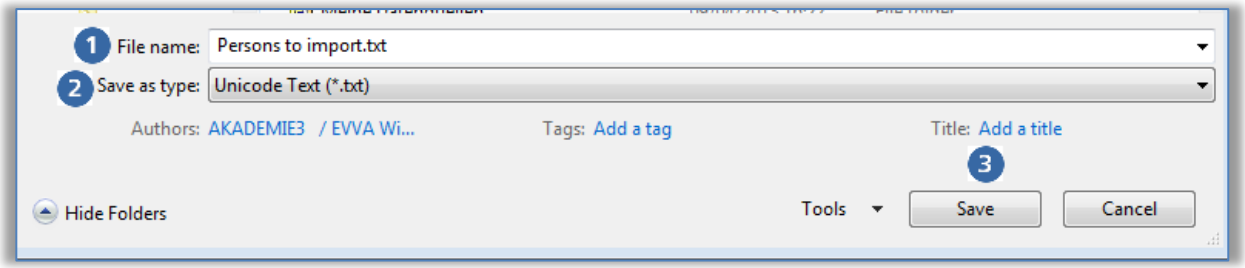
- Wadliwe wiersze w pliku CSV zostaną oznaczone symbolem ✖ i zostanie do nich dołączony tekst etykiety opisujący wszystkie błędy. Te wiersze nie zostaną zaimportowane.
- Niezależnie od ewentualnie występujących wierszy, wszystkie prawidłowe wiersze zostaną oznaczone symbolem ✔ oraz zaimportowane.

Kodowanie znaków w pliku CSV powinny odbywać się w standardzie UTF-8 – dzięki temu krajowe litery diakrytyczne (ą, ę, ł, Ä, ß, ç, Ñ, č itp.) będą prawidłowo wyświetlane. Utworzenie pliku CSV w formacie UTF-8 opisano szczegółowo w dalszej części.

Utworzenie pliku CSV w formacie UTF-8

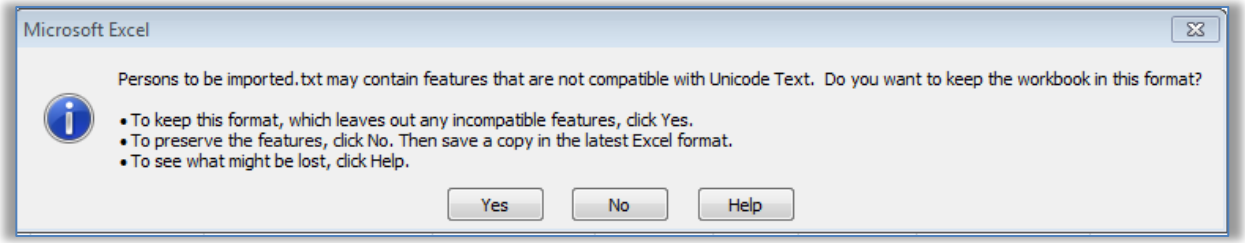
Poniższy opis dotyczy systemu Windows 10™ przy zastosowaniu programu Microsoft Excel™ oraz programów pomocniczych dostępnych w systemie Windows 10™. W przypadku innych wersji systemu Windows lub innych systemów operacyjnych utworzenie pliku CSV w formacie UTF-8 przebiega w podobny sposób. Niezbędne czynności:

- Sytuacją wyjściową w niniejszym opisie jest tabela Excel, która zawiera dane osób do zaimportowania.
- Należy upewnić się, że w arkuszu kalkulacyjnym Excel kolumna 7 (numer telefonu) jest sformatowana jako tekst. W razie przyjęcia formatu liczbowego znaki wprowadzające, takie jak "+" i "0" (zero), zostałaby utracone podczas konwersji. Spacje wewnątrz numeru telefonu są dozwolone i zwiększają czytelność danych w Module zarządzania online systemu AirKey.
- Za pomocą funkcji wyszukiwania w programie Excel należy sprawdzić, czy tabela nie zawiera następujących znaków:
  - " (podwójny, prosty cudzysłów)
  - ; (średnik = znak rozdzielający w pliku CSV, który ma zostać zaimportowany do Modułu zarządzania online systemu AirKey)
- Program Excel nie może zapisać danych bezpośrednio w formacie UTF-8. Dlatego najpierw należy koniecznie zapisać dane w formacie Unicode.
  - W tym celu w programie Excel należy otworzyć menu ***Plik*** → ***Zapisz jako*** (lub nacisnąć klawisz F12).
  - Pojawi się okno dialogowe i w polu "Zapisz jako" należy podać żądaną nazwę pliku ❶.
  - Z listy rozwijanej ***Typ pliku*** ❷ wybrać format ***Unicode Text (*.txt)***.
  - Kliknąć przycisk ***Zapisz*** ❸.



Rys. 32: Excel – Zapisz jako – "Unicode Text (*.txt)"

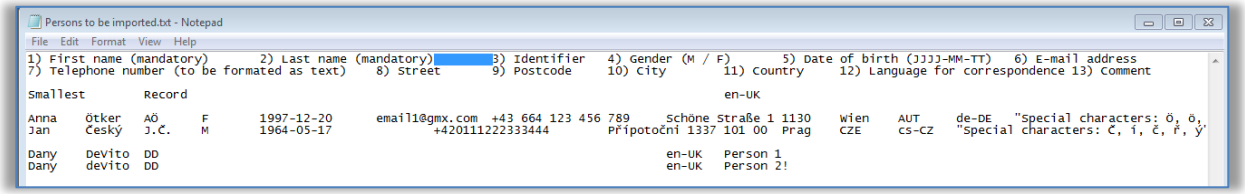
> Kolejne pytanie w programie Excel dotyczące opcji "Unicode Text" należy potwierdzić przyciskiem ***Tak***.



Rys. 33: Excel – Potwierdzenie zapisania jako "Unicode Text (*.txt)"

> Otworzyć w edytorze tekstu utworzony plik (*.txt). System Windows™ domyślnie użyje programu ***Edytor***.

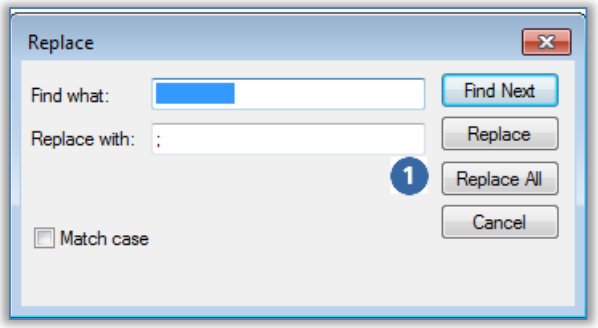
> Znakiem rozdzielającym w pliku tekstowym Unicode jest tabulator. Wszystkie tabulatory należy zastąpić średnikami (;). W tym celu najpierw należy zaznaczyć tabulator między 2 polami i skopiować go do schowka.



Rys. 34: Plik tekstowy w programie "Edytor" – zaznaczenie tabulatora i skopiowanie do schowka

> W programie ***Edytor*** otworzyć menu ***Edytuj*** → ***Zamień***, aby otworzyć okno dialogowe funkcji "Zamień".

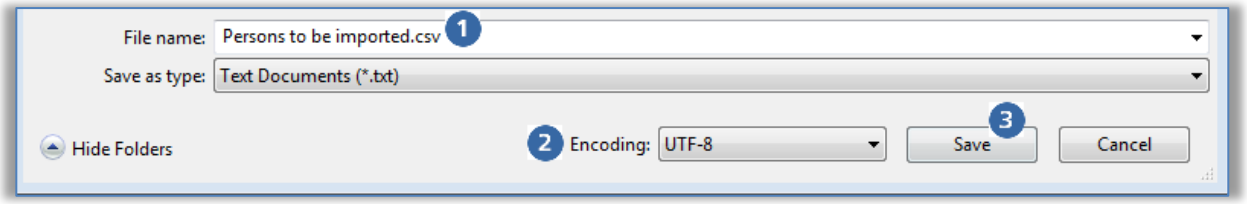
- W polu ***Szukaj*** należy wkleić znak tabulatora ze schowka, ponieważ tego znaku nie można wprowadzić tutaj bezpośrednio.
- W polu ***Zamień na*** wprowadzić średnik (;).
- Kliknąć przycisk ***Zamień wszystkie*** ❶.



Rys. 35: Program "Edytor" – zastąpienie wszystkich tabulatorów znakiem średnika

> Zamknąć okno dialogowe funkcji "Zamień" i w programie ***Edytor*** otworzyć menu ***Edytuj*** → ***Zapisz jako***, aby wyświetlić okno dialogowe funkcji "Zamień".

- Ręcznie zmienić rozszerzenie pliku z .txt na .csv w polu ***Nazwa pliku*** ❶. Późniejsza zmiana nazwy jest bardziej skomplikowana!
- Z listy rozwijanej ***Kodowanie*** ❷ wybrać format ***UTF-8***.
- Kliknąć przycisk ***Zapisz*** ❸.



Rys. 36: Program "Edytor" – Zapisz jako – ręczne wprowadzenie rozszerzenia .csv i wybór kodowania UTF-8

> Utworzony w ten sposób plik CSV można następnie zaimportować do Modułu zarządzania online systemu AirKey.

Plik CSV można bezpośrednio otworzyć w programie Excel. Proszę nie wprowadzać ŻADNYCH zmian w pliku CSV w programie Excel, ponieważ podczas zapisywania kodowanie UTF-8 zostanie zmienione!

Niewielkie, późniejsze zmiany danych osobowych można wprowadzić w pliku CSV, gdy plik będzie otwarty i zapisany np. za pomocą programu ***Edytor***.

W razie bardziej złożonych zmian danych osobowych zalecamy, aby dopasować dane w pierwotnym pliku Excel i powtórzyć całą procedurę utworzenia pliku CSV w formacie UTF-8.

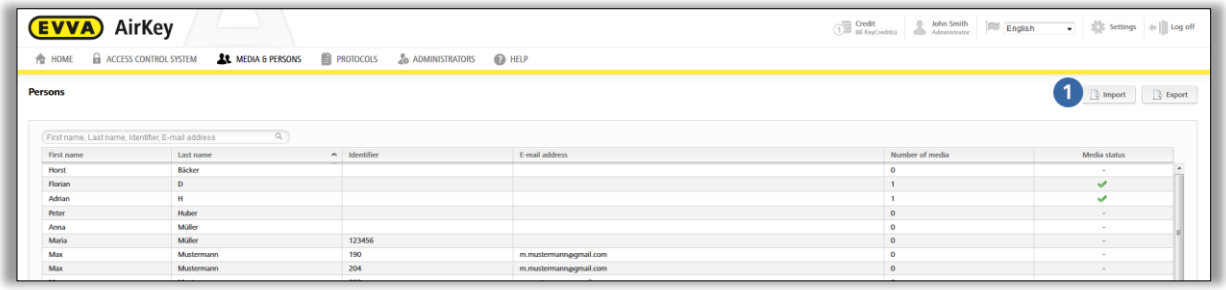
Importowanie pliku CSV w formacie UTF-8 do Modułu zarządzania online systemu AirKey

Aby zaimportować plik CSV z danymi osobowymi, należy wykonać następującą procedurę:

> Na stronie startowej ***Home*** wybrać ikonę ***Osoby***.

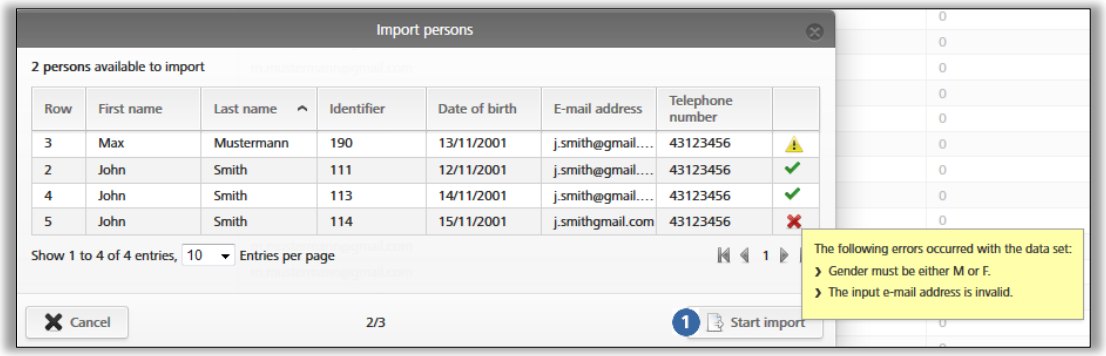
> Alternatywnie w menu głównym wybrać opcję ***Nośniki i osoby*** → ***Osoby***.

> Z prawej strony ekranu kliknąć przycisk ***Importuj*** ❶.



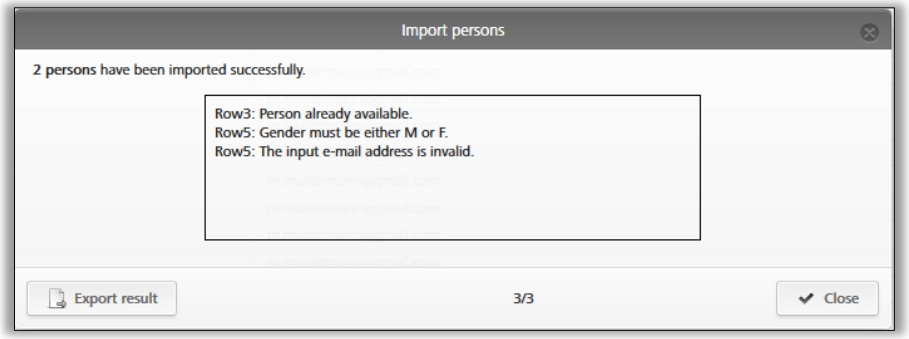
Rys. 37: Importowanie osób

- Wybrać opcję ***Wybierz plik.***
- Wybrać plik CSV do zaimportowania.
- Pojawi się przegląd osób do zaimportowania.
- Kliknąć opcję ***Rozpocznij import*** ❶.



Rys. 38: Importowanie osób

- Pojawi się komunikat o liczbie pomyślnie zaimportowanych osób oraz o liczbie wadliwych wierszy.
- Kliknąć opcję ***Zamknij***.



Rys. 39: Importowanie osób – rezultat

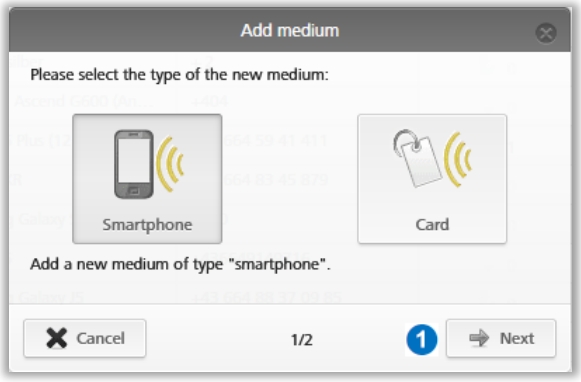
- Nastąpi automatyczne przejście do listy przeglądu osób w Module zarządzania online systemu AirKey.
- Aby przyporządkować żądane uprawnienia dostępu danej osobie, można to wykonać dla każdej poszczególnej osoby zgodnie z opisem w rozdziale Przypisanie nośnika do osoby. Identyczne uprawnienia dostępu można szybko i prosto powielać za pomocą

funkcji duplikacji. Informacje na ten temat można znaleźć w rozdziale Kopiowanie nośnika.

4.8 Utworzenie smartfona

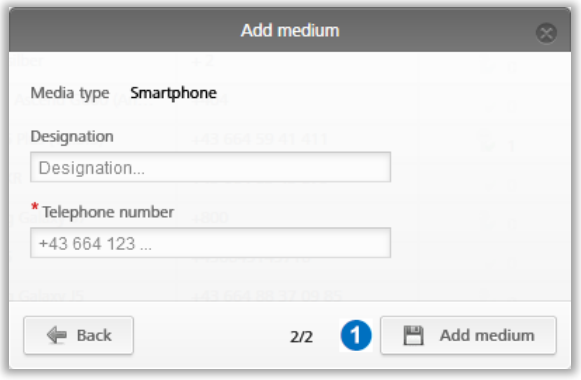
Aby zarządzać smartfonami w ramach systemu zamknięć, najpierw należy je utworzyć w systemie lub dodać do systemu.

- Na stronie startowej ***Home*** na szarym pasku bloku ***Nośniki i osoby*** kliknąć ***Dodaj*** → ***Dodaj nośnik***.
- Alternatywnie można wybrać na stronie startowej ***Home*** ikonę ***Smartfony*** → ***Dodaj nośnik***.
- Alternatywnie w menu głównym można wybrać opcje ***Nośniki i osoby*** → ***Dodaj nośnik***.



Rys. 40: Nowy nośnik – smartfon lub karta

- Wybrać ***Smartfon*** jako nowy nośnik i kliknąć przycisk ***Dalej*** ❶.
- W polu "Oznaczenie" wprowadzić istotne informacje (np. typ smartfona).
- Wprowadzić numer telefoniczny smartfona. Numer telefonu musi zaczynać się od znaku **+** i numeru kierunkowego kraju, i może zawierać maksymalnie 50 znaków (+, 0-9 i spacje).
- Kliknąć opcję ***Dodaj nośnik*** ❶.

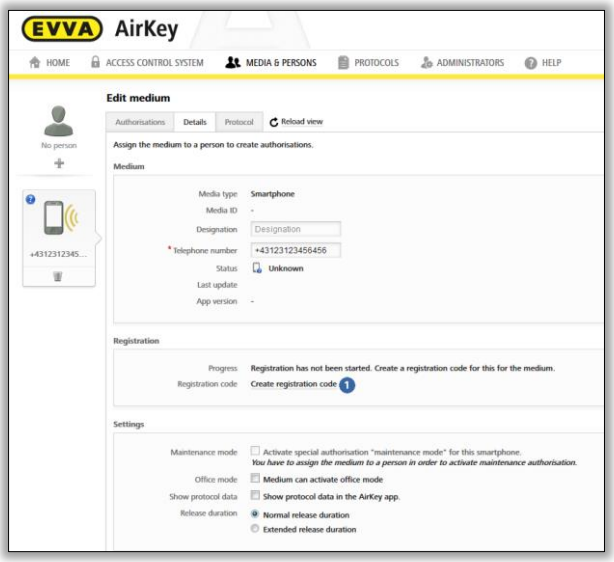


Rys. 41: Utworzenie nowego nośnika

Jeśli numer telefonu jest nieprawidłowy lub został już utworzony nośnik z tym numerem, zostanie wyświetlony komunikat błędu.

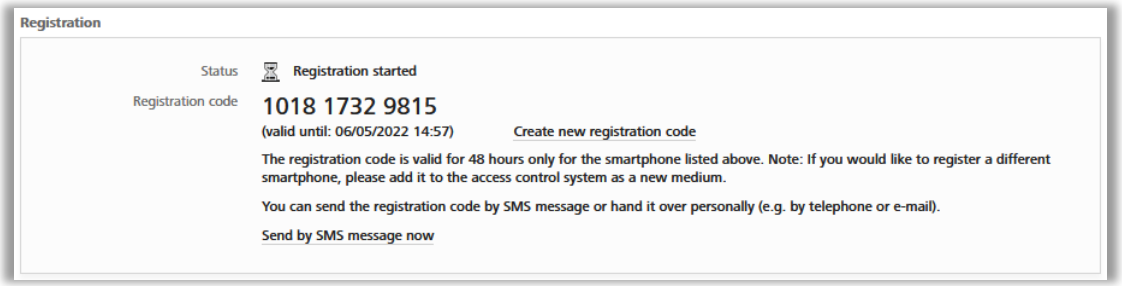
Teraz użytkownik zostanie przełączony do pola "Szczegóły" danego smartfona.

> Kliknąć opcję ***Utwórz kod rejestracji*** ❶, jeśli nie został jeszcze utworzony kod rejestracji.



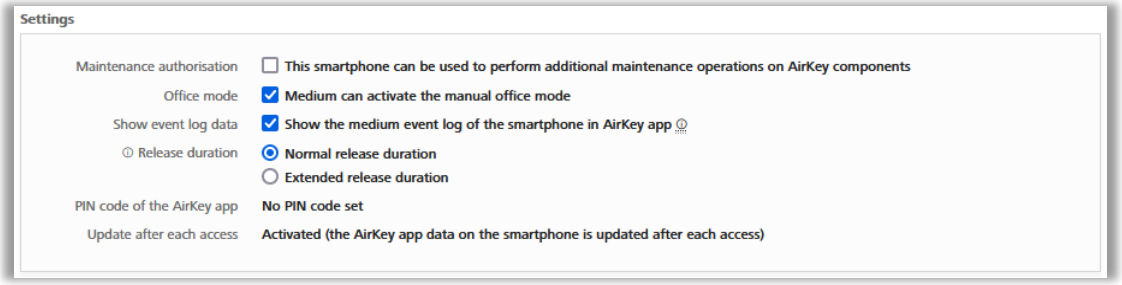
Rys. 42: Utworzenie kodu rejestracji

W bloku ***Rejestracja*** będzie wyświetlony ważny kod rejestracji z okresem ważności. Można go także przesłać za pośrednictwem wiadomości SMS. W tym celu należy kliknąć odpowiedni link. Wówczas zostanie wyświetlona dokładna data i godzina wysłania kodu rejestracji poprzez wiadomość SMS.



Rys. 43: Kod rejestracji

W bloku ***Ustawienia*** w ramach szczegółów danego smartfona można określić następujące ustawienia:



Rys. 44: Edycja nośnika – ustawienia

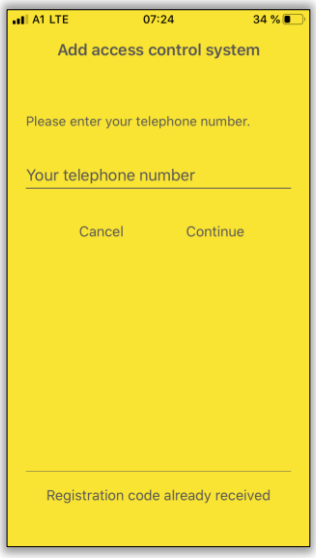
- **Uprawnienie do konserwacji:** To specjalne uprawnienie można aktywować tylko w przypadku tego smartfona, który został już przypisany osobie. Dzięki tej funkcji smartfon uzyskuje uprawnienia do blokowania komponentów zamykających w stanie fabrycznym, a także do usuwania/dodawania komponentów zamykających i nośników do systemu AirKey. Ponadto może dokonywać aktualizacji firmware komponentów zamykających i programu Keyring nośników.
- **Ten nośnik może aktywować ręczne stałe otwarcie:** Jeśli ta opcja zostanie wybrana, nośnik dostępu może przełączać komponent zamykający w stan automatycznego stałego otwarcia. Jednak nośnik musi mieć ważne uprawnienie dla danego komponentu zamykającego.
- **Wyświetl protokół nośnika smartfona w aplikacji AirKey:** Za pomocą tej opcji osoba może wyświetlić w aplikacji AirKey swoje zdarzenia dostępu oraz inne istotne dane z protokołów, dotyczące nośnika określonej osoby.
- **Okres zezwolenia:** Ustawienie definiuje czas odblokowania komponentu zamykającego aż do jego zablokowania dla danego smartfona. Długości normalnego lub rozszerzonego okresu zezwolenia są definiowane dla komponentu zamykającego (zakres 1-250 sekund).
- **Kod PIN aplikacji AirKey:** Ustawienie wskazuje, czy dla tego smartfona w aplikacji AirKey aktywowano blokadę kodu PIN lub nie. Jeśli blokada została aktywowana a osoba zapomniała swojego kodu PIN, można go tutaj ewentualnie zresetować.
- **Aktualizacja po każdym dostępie:** Podaje status, czy dane aplikacji AirKey tego smartfona są automatycznie aktualizowane po każdej operacji dostępu. Szczegóły dotyczące uaktualniania tej funkcji znajdziesz w rozdziale Informacje ogólne.

4.9 Rejestracja smartfona

Smartfon można zarejestrować, jeśli został on utworzony w ramach systemu zamknięć i użytkownik zna kod rejestracji.

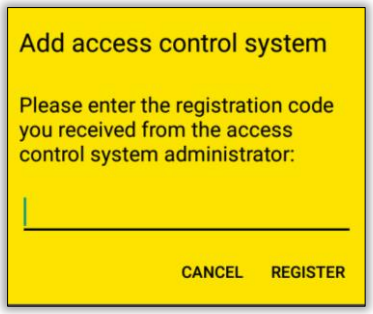
- Uruchomić aplikację AirKey na swoim smartfonie.
- Zaakceptuj postanowienia licencyjne oraz potwierdź ewentualne pytania dotyczące dostępu do określonych usług w smartfonie.
- Jeśli smartfon nie został powiązany z żadnym systemem zamknięć, automatycznie zostanie wyświetlone okno dialogowe wprowadzania kodu rejestracji.

W przypadku smartfonów z systemem iOS należy wybrać opcję ***Już otrzymano kod rejestracji***, aby pominąć wprowadzanie numeru telefonu i przejść do wprowadzania kodu rejestracji.



Rys. 45: Aplikacja AirKey — dodawanie systemu zamknięć (iOS)

> Wprowadzić kod rejestracji otrzymany od administratora systemu zamknięć AirKey.
> Potwierdzić wprowadzoną wartość, naciskając przycisk ***Zarejestruj***.



Rys. 46: Aplikacja AirKey – dodawanie systemu zamknięć

Jeden smartfon można zarejestrować także w kilku systemach AirKey. Aby ponownie otworzyć okno dialogowe rejestracji, wybrać w menu głównym aplikacji AirKey opcję ***Ustawienia*** → ***Dodaj system zamknięć***. Bliższe informacje na ten temat można znaleźć w rozdziale Używanie smartfona w kilku systemach.

Jeśli kod rejestracji jest nieprawidłowy lub upłynął jego okres ważności, zostanie wyświetlony komunikat błędu. W takim przypadku należy zwrócić się do administratora systemu zamknięć, który przekazał kod rejestracji.

Jeśli aplikacja AirKey lub dane aplikacji zostały usunięte, istnieje możliwość przesłania już przyznanych uprawnień na smartfon bez użycia kredytu jednostek. Dotyczy to jednak tylko tego samego urządzenia i danego systemu zamknięć. W razie zamiany urządzeń nie będzie to możliwe.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony***.
- Alternatywnie w lewym wierszu nagłówka można wybrać opcje ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć wybrany smartfon.
- Kliknąć opcję ***Utwórz nowy kod rejestracji*** i przekazać wygenerowany kod rejestracji osobie, która zamierza zarejestrować swój smartfon w systemie zamknięć. Albo wyślij je bezpośrednio do smartfona jako wiadomość SMS.
- Wprowadzić kod rejestracji do aplikacji AirKey – smartfon zostanie zarejestrowany w systemie zamknięć.

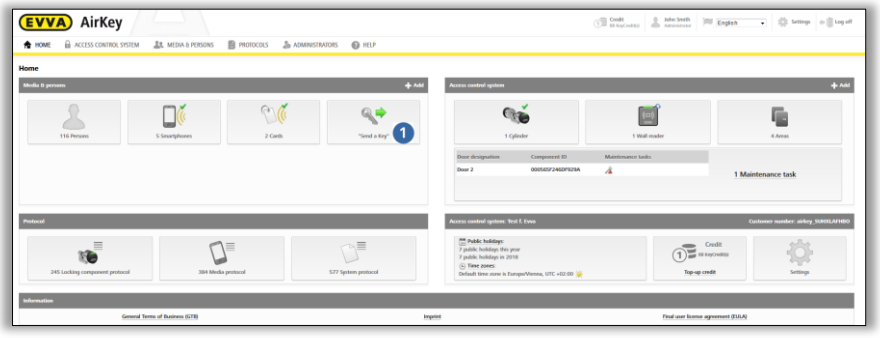
Jeśli dany smartfon był już zarejestrowany w systemie AirKey, nie został prawidłowo z niego usunięty, dane aplikacji lub aplikacja AirKey została usunięta a smartfon ma być zarejestrowany w innym systemie zamknięć AirKey, pojawi się komunikat informujący o tym, że smartfon został już zarejestrowany w systemie AirKey. Jeśli komunikat zostanie zignorowany, smartfon można zarejestrować w normalny sposób. Zostanie on utworzony w systemie jako nowy nośnik, a wszystkie dotychczasowe dane nie będą nadawać się do użytku.

Firma EVVA zaleca stosowanie kodu PIN. Służy on jako dodatkowy poziom zabezpieczenia i można go w późniejszym okresie aktywować lub dezaktywować. Bliższe informacje na ten temat można znaleźć w rozdziale Aktywowanie kodu PIN.

4.9.1 Funkcja "Send a Key"

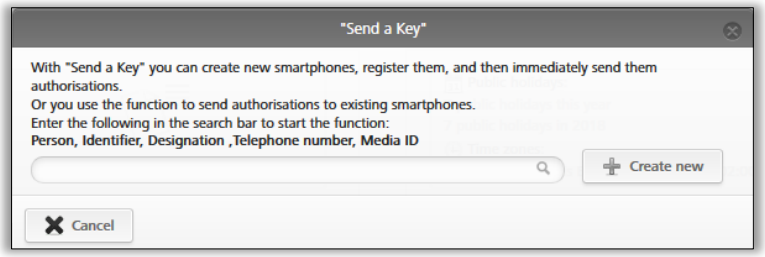
Do wszystkich osób, które posiadają smartfona, "klucz" można wysłać także poprzez funkcję "Send a Key". Z tej funkcji może korzystać administrator, co zaoszczędzi właścicielowi smartfona ręcznego wprowadzania kodu rejestracji do nowego systemu zamknięć.

- Kliknąć przycisk **"*Send a Key*""**.



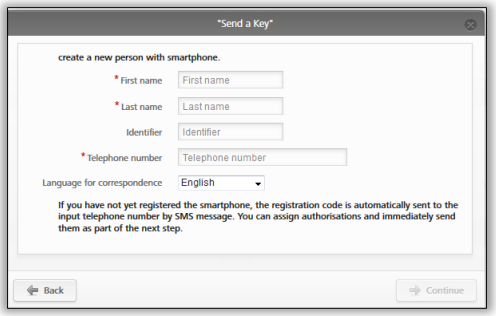
Rys. 47: "Send a Key"

- W polu wyszukiwania podać nazwę osoby, identyfikator itp. Jeśli dana osoba nie została jeszcze utworzona w systemie, należy wybrać opcję ***Utwórz nowy***.



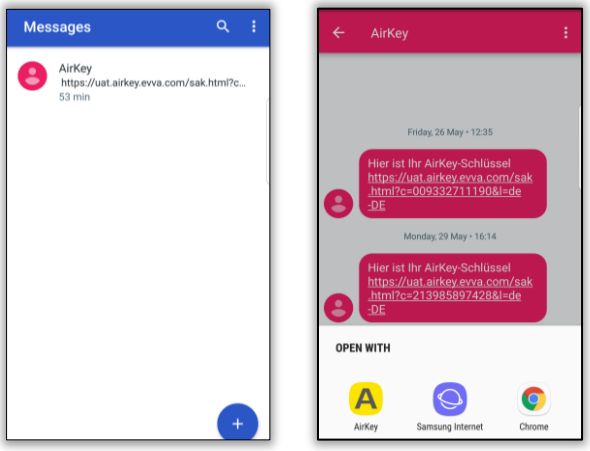
Rys. 48: "Send a Key" – pole wyszukiwania

> Po wypełnieniu wszystkich pól obowiązkowych kliknąć ***Dalej.*** Do określonej osoby natychmiast zostanie wysłana wiadomość SMS zawierająca link z kodem rejestracji do aplikacji AirKey.



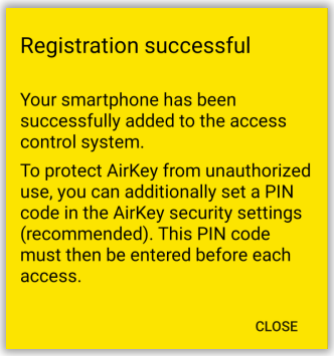
Rys. 49: "Send a Key" – utworzenie osoby

W zależności od dostępności sieci smartfona otrzymanie wiadomości SMS z kodem rejestracji może trochę potrwać.



Rys. 50: SMS z linkiem – tu pokazano na ekranie Samsung Galaxy S7 Edge

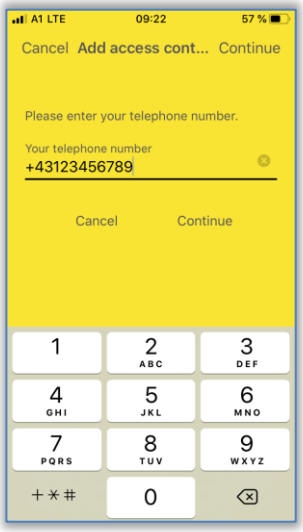
> Po uruchomieniu linku z wiadomości SMS za pomocą AirKey zostanie automatycznie zainicjowana i przeprowadzona rejestracja.



Rys. 51: Rejestracja udana

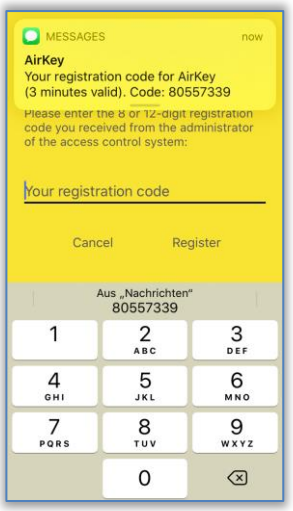
Jeśli aplikacja mobilna AirKey jeszcze nie została zainstalowana na smartfonie, obowiązuje następujący sposób postępowania:

- Kliknij link w wiadomości SMS i zainstaluj aplikację na smartfonie.
- Uruchom aplikację AirKey.
- W przypadku smartfonów z systemem Android rejestracja zostanie automatycznie zainicjowana i przeprowadzona. W przypadku smartfonów z systemem iOS należy wprowadzić swój numer telefonu i potwierdzić przyciskiem ***Kontynuuj***.



Rys. 52: Wprowadzanie numeru telefonu (iOS)

- Otrzymasz następną wiadomość SMS. Pozostań w aplikacji AirKey i wybierz ośmioznakowy kod rejestracji, który zostanie wyświetlony nad klawiaturą.

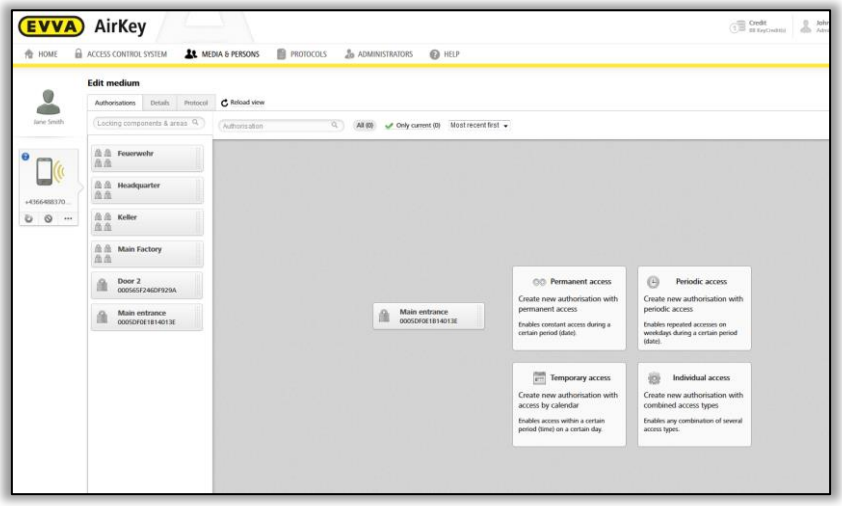


Rys. 53: Kod rejestracji (iOS)

Jeśli ośmioznakowy kod rejestracji nie będzie wyświetlony jako propozycja lub gdy w międzyczasie aplikacja AirKey została zamknięta, należy skopiować ośmioznakowy kod rejestracji z SMS-a i wkleić w aplikacji AirKey.

> Zakończ rejestrację przyciskiem ***Zarejestruj***.

Po użyciu funkcji "Send a Key", w module zarządzania online nastąpi przejście do widoku uprawnień ***Edytuj nośnik***, gdzie można utworzyć żądane uprawnienia. Metodą "przeciągnij i upuść" przesunąć określone komponenty zamykające, dla których ma zostać przyznane uprawnienie dostępu, do wybranego rodzaju dostępu (Stały dostęp, dostęp tymczasowy, dostęp okresowy, dostęp indywidualny) – patrz także rozdział Przydzielanie uprawnień.



Rys. 54: Rodzaje dostępu

4.10 Instalacja komponentów zamykających

4.10.1 Wkładka AirKey

Przy montażu wkładki AirKey, wkładki hybrydowej, zamka gwintowanego z ryglem i kłódki AirKey. Przestrzegaj dołączonej do opakowania instrukcji montażu albo instrukcji montażu wideo dostępnej online pod adresem https://www.evva.com/pl/airkey/website/.

W przypadku wkładki AirKey z obustronnym dostępem należy pamiętać o tym, aby w systemie zamknięć AirKey zostały skonfigurowane obydwie strony. W ten sposób można uniknąć niezamierzonego zablokowania drzwi.

4.10.2 Czytnik naścienny AirKey

Podczas montażu czytnika naściennego AirKey należy przestrzegać instrukcji montażu dołączonej do opakowania. Dodatkowo na naszej stronie internetowej można znaleźć szablon otworowania lub film na temat montażu pod adresem https://www.evva.com/pl/airkey/website/.

Na każdy czytnik naścienny potrzebna jest jedna centralka sterująca. Centralkę sterującą należy zamontować w bezpiecznym miejscu wewnątrz budynku. Należy skontrolować okablowanie czytnika naściennego i centralki sterującej.

Komponenty zamykające AirKey są zawsze dostarczane w stanie fabrycznym.

Nośniki w stanie fabrycznym blokują komponenty zamykające w stanie fabrycznym.

- Smartfony z zainstalowaną aplikacją AirKey i uprawnieniem do trybu konserwacji blokują komponenty zamykające w stanie fabrycznym.
- W stanie fabrycznym nie odbywa się zapis prób blokowania.
- Uprawnienie do zamykania będzie dostępne dopiero wówczas, gdy komponent zamykający AirKey będzie dodany do systemu zamknięć.
- Podczas montażu należy przestrzegać wskazówek zawartych w instrukcji montażowej. Podczas montażu lub demontażu komponentów zamykających należy otworzyć drzwi i unieruchomić je, tak aby nie zamknęły się przypadkowo.

4.11 Dodawanie komponentu zamykającego

Komponenty zamykające można dodawać do systemu zamknięć za pomocą smartfona z uprawnieniem do trybu konserwacji lub za pomocą opcjonalnej stacji kodującej. Te komponenty muszą znajdować się w stanie fabrycznym.

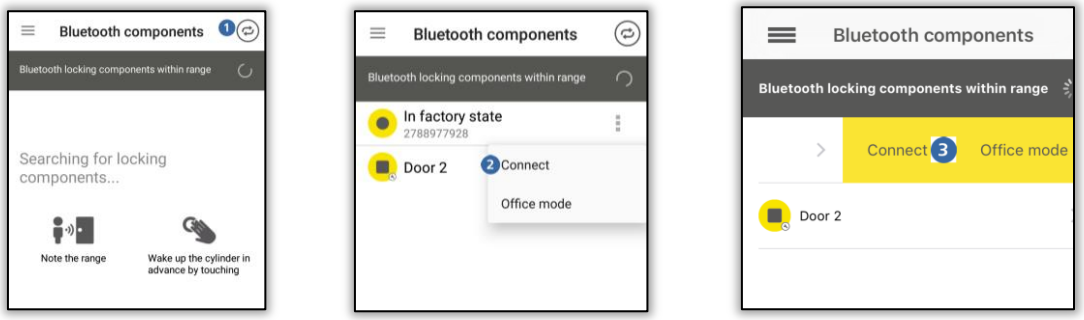
Aby zastosować do tego celu smartfon, należy spełnić poniższe warunki:

- Aplikacja AirKey została zainstalowana.
- Dostępne jest aktywne połączenie z Internetem.
- Smartfon został zarejestrowany w określonym systemie zamknięć.

- Smartfon został przypisany do określonej osoby.
- Do smartfona przypisano uprawnienie konserwacyjne.

4.11.1 Dodawanie komponentu zamykającego za pomocą smartfona

- Uruchomić aplikację AirKey.
- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.
- Utworzenie połączenia **Bluetooth** (w smartfonach z systemem **Android**): W menu kontekstowym wybrać komponent zamykający w stanie fabrycznym, który ma być dodany do systemu zamknięć (⋮), a następnie wybrać opcję ***Połącz*** ❷.
- Utworzenie połączenia **Bluetooth** (w urządzeniach **iPhone**): Przesunąć komponent zamykający w stanie fabrycznym, który ma być dodany do systemu zamknięć i który ma oznaczenie "W stanie fabrycznym", w lewo, a następnie wybrać opcję ***Połącz*** ❸.



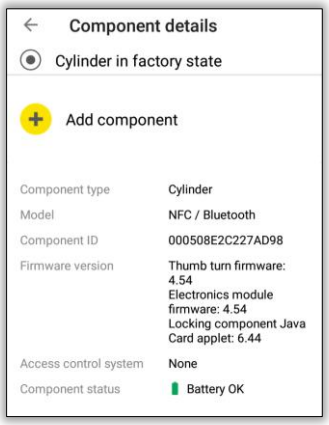
Rys. 55: Aplikacja AirKey – *połączenie z komponentem* (NFC dla smartfonów Android, Bluetooth dla smartfonów Android, Bluetooth dla iPhone'a)

Rys. 56: Aplikacja AirKey – połączenie z komponentem

- Przytrzymaj smartfon przy komponencie zamykającym w stanie fabrycznym (w razie połączenia NFC), aby utworzyć połączenie. Połączenie przez Bluetooth jest nawiązywane automatycznie. W żadnym razie nie wolno odsuwać smartfona od komponentu zamykającego podczas nawiązywania połączenia.

Rys. 57: Aplikacja AirKey – nawiązywanie połączenia

> Zostaną wyświetlone informacje na temat komponentu zamykającego.



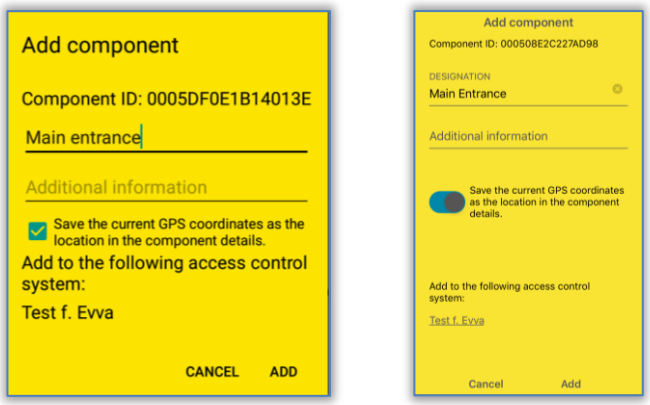
Rys. 58: Dodawanie komponentu

> Nacisnąć przycisk ***Dodaj komponent.***

> Wprowadzić zrozumiałe oznaczenie komponentu zamykającego.

W przypadku wkładki z obustronnym dostępem należy pamiętać o tym, aby w systemie AirKey zostały skonfigurowane obydwie strony. Obie strony wkładki należy nazwać za pomocą zrozumiałego oznaczenia. Należy utworzyć strefę, do którego będą należeć obie strony wkładki i przypisać uprawnienie strefowe, aby dla obydwu stron otrzymać identyczne uprawnienia.

> Jeśli smartfon jest zarejestrowany w kilku systemach zamknięć z aktywnym trybem konserwacji, należy wybrać system zamknięć, do którego ma zostać dodany komponent zamykający.



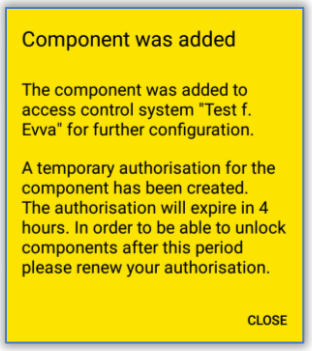
Rys. 59: Aplikacja AirKey – dodawanie komponentu zamykającego (Android / iPhone)

> Nacisnąć przycisk ***Dodaj***.

> Jeszcze raz przytrzymaj smartfon przy komponencie zamykającym w stanie fabrycznym (w razie połączenia NFC); aby nawiązać połączenie. Połączenie przez Bluetooth jest nawiązywane automatycznie.

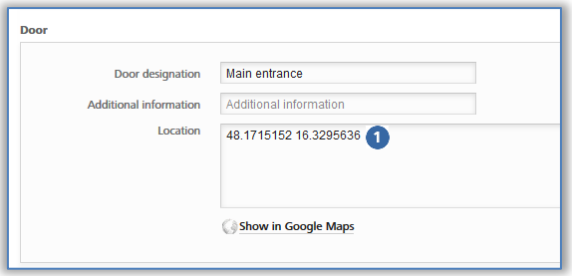
Nastąpi sprawdzenie danych i komponent zamykający zostanie zaktualizowany. Podczas tego procesu nie wolno oddalać smartfona od komponentu zamykającego.

> Operacja zostanie potwierdzona komunikatem o pomyślnym ukończeniu. Komponent zamykający będzie teraz dostępny w Module zarządzania online systemu AirKey do dalszych czynności administracyjnych.



Rys. 60: Aplikacja AirKey – komponent zamykający został dodany

Komponent zamykający pojawi się na liście przeglądu komponentów zamykających w Module zarządzania online systemu AirKey. Jeśli podczas dodawania komponentu zamykającego zostały ustalone współrzędne GPS ❶, można je znaleźć w module zarządzania online dla danego komponentu zamykającego w zakładce ***Szczegóły*** w bloku "Drzwi".



Rys. 61: Współrzędne GPS w szczegółach komponentu zamykającego

Alternatywnie w polu "Lokalizacja" można wprowadzić adres, który określa miejsce komponentu zamykającego.

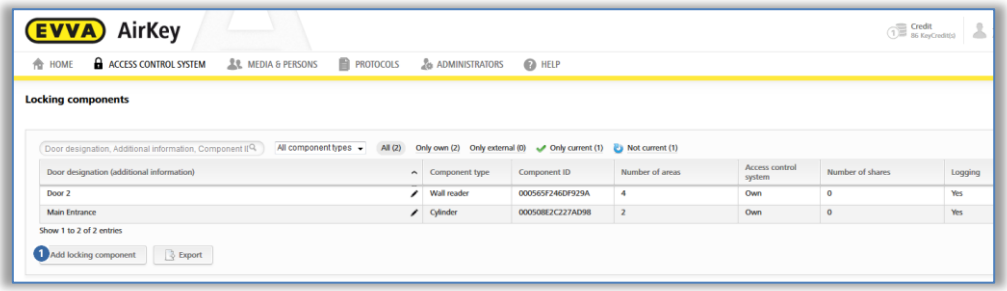
Komponent zamykający nie jest już w stanie fabrycznym. Nośniki w stanie fabrycznym ani smartfony w trybie konserwacji nie mają już uprawnień do jego obsługi. Smartfon, za pomocą którego dodano komponent zamykający, będzie automatycznie uprawniony do obsługi danego komponentu przez okres 4 godzin. Należy w porę zmienić te uprawnienie lub przypisać ważne uprawnienie innym nośnikom, aby zachować dostęp do tego komponentu zamykającego.

4.11.2 Dodawanie komponentu zamykającego za pomocą stacji kodującej

Option

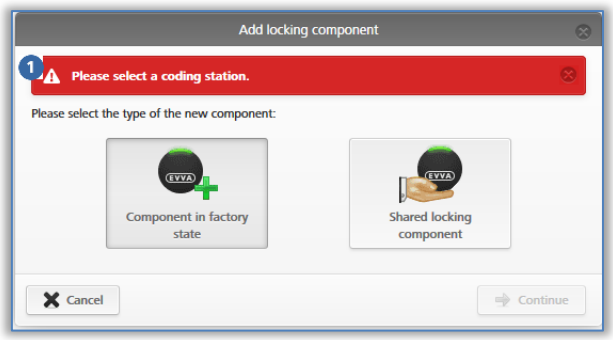
Aby dodać komponent zamykający za pomocą stacji kodującej, należy wykonać poniższe czynności:

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Kliknąć przycisk ***Dodaj komponent zamykający*** 1.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.



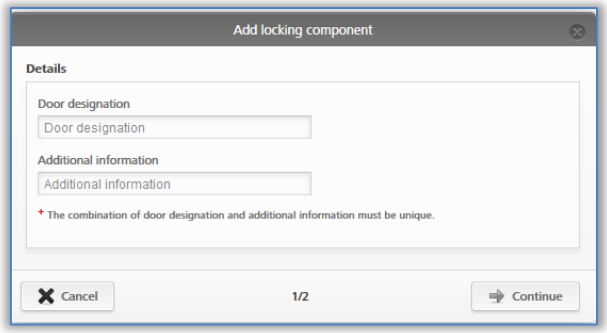
Rys. 62: Dodawanie komponentu zamykającego

- Podłączyć stację kodującą do komputera; w przeciwnym razie pojawi się komunikat systemowy 1.



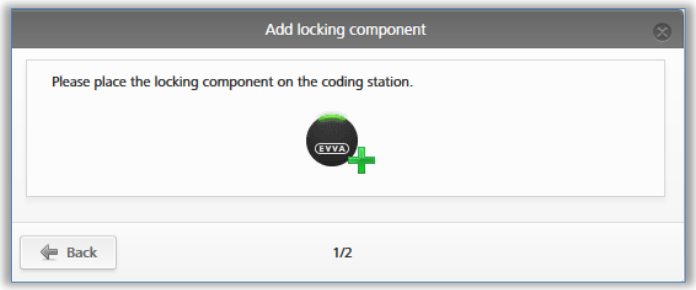
Rys. 63: Dodawanie komponentu zamykającego / brak stacji kodującej

- Wybrać opcję ***Komponent w stanie fabrycznym.***
- Kliknąć przycisk ***Dalej***.
- W następnym oknie dialogowym wprowadzić oznaczenie drzwi i kliknąć przycisk ***Dalej.***



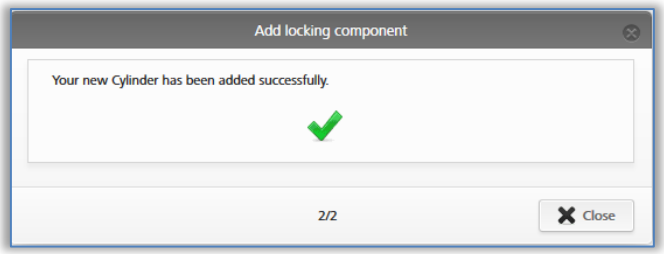
Rys. 64: Dodawanie komponentu zamykającego – określanie nazwy

- Postępować zgodnie z instrukcjami i położyć komponent zamykający na stacji kodującej.



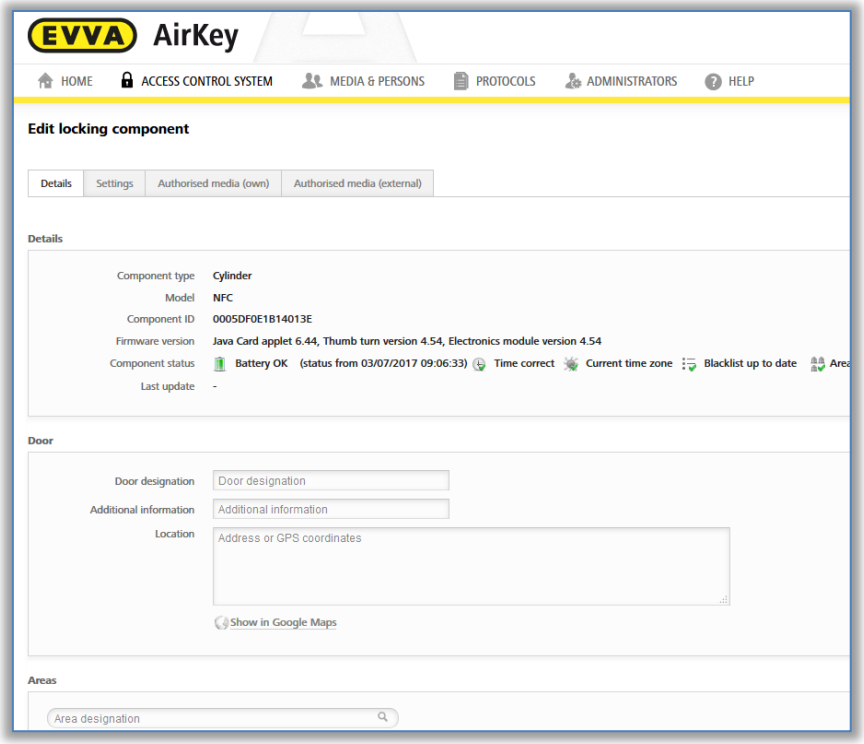
Rys. 65: Dodawanie komponentu zamykającego

- Pojawi się komunikat informujący o pomyślnym dodaniu komponentu zamyka–jącego systemu AirKey.



Rys. 66: Dodawanie komponentu zamykającego – komunikat potwierdzający

Po zamknięciu komunikatu informującego o pomyślnym wykonaniu operacji nastąpi przełączenie do widoku szczegółów danego komponentu zamykającego.



Rys. 67: Szczegóły komponentu zamykającego

Komponent zamykający nie jest już w stanie fabrycznym. Nośniki w stanie fabrycznym ani smartfony z uprawnieniem do konserwacji nie mają już uprawnień do jego odryglowania. Dodać nośnik lub smartfon do systemu zamknięć oraz przydzielić ważne uprawnienie dla komponentu zamykającego, aby możliwe było jego ryglowanie i odryglowanie.

Domyślna strefa czasowa i ustawienia dotyczące ochrony danych dla komponentu są automatycznie konfigurowane w zależności od przyjętych ustawień. Bliższe informacje na temat tych ustawień można znaleźć w rozdziale Wartości domyślne dla wszystkich nowo dodanych komponentów zamykających.

Alternatywnie można także umieścić komponent zamykający w stanie fabrycznym na stacji kodującej. Na dole, z prawej strony ekranu pojawi się okno informacyjne i aby dodać komponent zamykający do systemu AirKey, należy skorzystać z opcji ***Dodaj komponent do mojego systemu zamknięć***.

Rys. 68: Dodawanie komponentu do własnego systemu zamknięć

4.12 Dodawanie kart, breloków do kluczy, bransoletki i kluczy Combi za pomocą smartfona

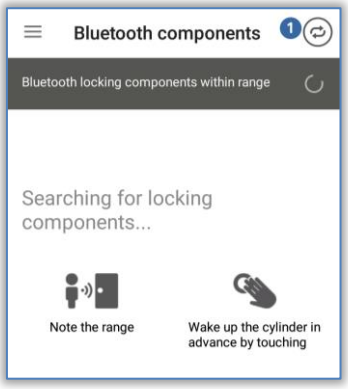
Nośniki dostępu w stanie fabrycznym są dodawane do systemu AirKey za pomocą smartfona z uprawnieniem konserwacyjnym lub opcjonalnej stacji kodującej.

> Uruchomić aplikację AirKey.

Aby dodać klucz Combi za pomocą smartfona, należy przytrzymać przy smartfonie klucz Combi z tej strony, na której znajduje się symbol RFID. W większości modeli należy przytrzymać klucz Combi bezpośrednio przy smartfonie.

Tę czynność można wykonać tylko przy użyciu smartfona z systemem Android, obsługującego technologię NFC. W kwestii dodawania nośników poprzez połączenie Bluetooth smartfona Android lub iPhone'a – patrz rozdział Kodowanie nośników.

> Nacisnąć symbol ***Połącz z komponentem*** ❶.

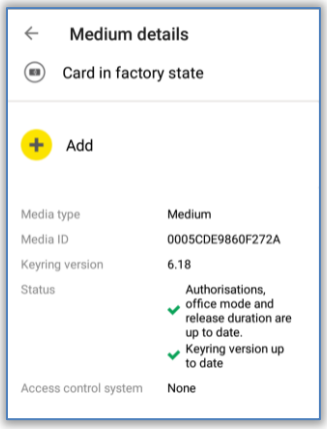


Rys. 69: Aplikacja AirKey – połączenie z komponentem

> Przytrzymać smartfon przy nośniku w stanie fabrycznym.
Zostanie nawiązane połączenie z nośnikiem.

Rys. 70: Aplikacja AirKey – nawiązywanie połączenia

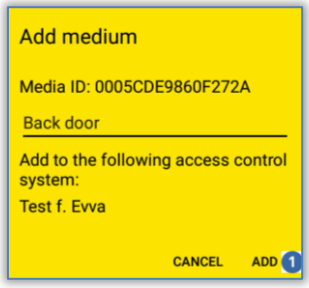
> W żadnym razie nie wolno odsuwać nośnika od smartfona podczas nawiązywania połączenia. Zostaną wyświetlone informacje na temat nośnika.



Rys. 71: Szczegóły nośnika

> Nacisnąć przycisk ***Dodaj***.

> Wprowadzić oznaczenie nośnika.



Rys. 72: Dodawanie nośnika – ustalanie nazwy

> Jeśli smartfon jest zarejestrowany w kilku systemach zamknięć, należy wybrać system zamknięć, do którego ma zostać dodany nośnik.

> Nacisnąć przycisk ***Dodaj*** ❶.

> Ponownie przytrzymać smartfon przy nośniku, aby zakończyć operację.

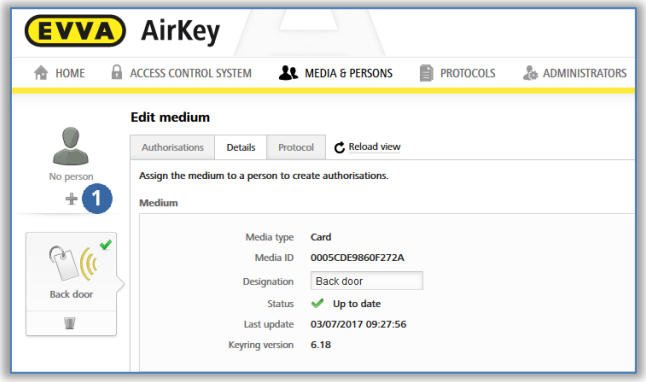
> Operacja zostanie potwierdzona komunikatem o pomyślnym ukończeniu. Nośnik jest teraz dostępny w Module zarządzania online systemu AirKey i należy go jeszcze przypisać do określonej osoby.

Ta operacja wygląda identycznie w przypadku kart, breloków do kluczy, bransoletki i kluczy Combi. Wszystkie trzy rodzaje nośników są traktowane przez system również jako "karta".

4.13 Przypisanie nośnika do osoby

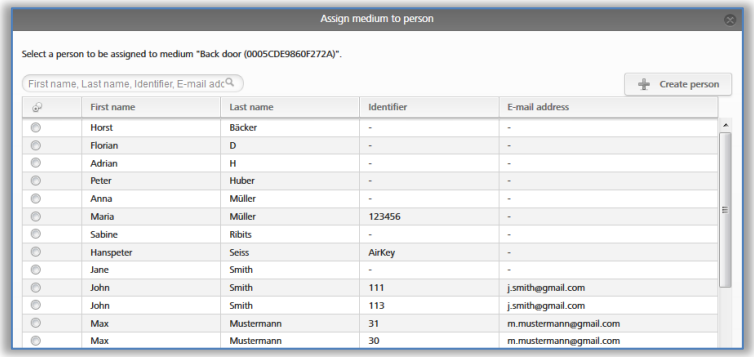
Kolejnym krokiem jest przypisanie nośnika wybranej osobie w Module zarządzania online systemu AirKey, aby możliwe było przyznanie uprawnień. Tylko w ten sposób można uzyskać relację osobową w przypadku dostępów.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście nośników wybrać ten nośnik, który jeszcze nie został przypisany do żadnej osoby.
- Przy wskazaniu ***Brak osoby*** kliknąć symbol **+** ❶



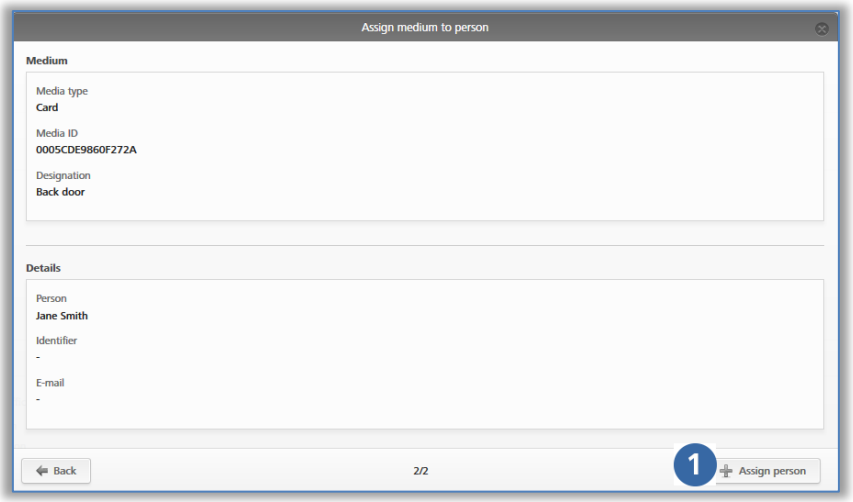
Rys. 73: Przypisanie osoby

- Z listy osób wybrać osobę, do której zostanie przypisany nośnik.



Rys. 74: Przypisanie osoby do nośnika

- Jeśli żądana osoba jeszcze nie została utworzona, dostępny jest przycisk ***Utwórz osobę***, po naciśnięciu którego użytkownik przejdzie do drugiego okna dialogowego "Przypisanie nośnika do osoby".
- Zatwierdzić wybraną osobę, której zostanie przypisany nośnik za pomocą opcji ***Przypisz osobę*** ❶.



Rys. 75: Zatwierdzenie wyboru osoby

> Dalsze czynności – patrz rozdział Przydzielanie uprawnień.

Alternatywnie można wykonać przypisanie nośnika danej osobie za pomocą danych nośnika. Bliższe informacje na ten temat znajdują się w rozdziale Przypisanie nośnika do osoby.

4.14 Przydzielanie uprawnień

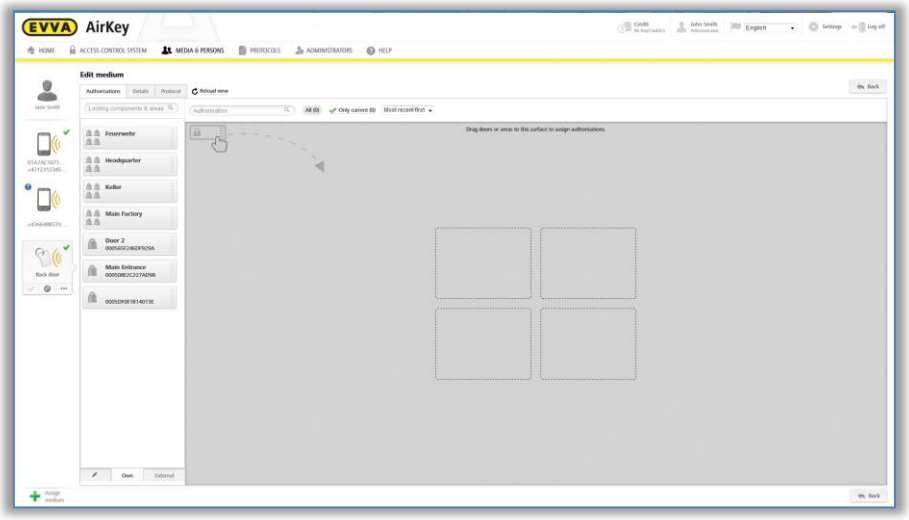
Należy pamiętać, że uprawnienia można przydzielać dopiero wówczas, gdy nośnik został przypisany danej osobie.

> Wybrać w menu głównym opcje ***Nośniki i osoby*** → ***Nośniki***.

> Na liście przeglądu kliknąć żądany nośnik.

> Jeśli nośnik został przypisany do osoby, pojawi się przegląd uprawnień nośnika.

> Gdy odpowiedni komponent zamykający zostanie wybrany i przeciągnięty na szare pole, pojawią się możliwe rodzaje dostępów w czterech polach w obwódce punktowej.



Rys. 76: Przydzielanie uprawnień

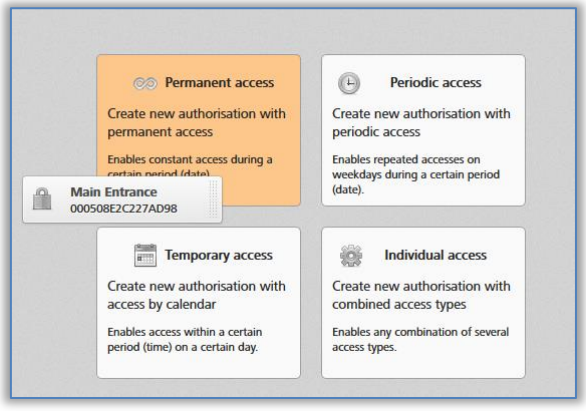
> Wybrać żądany rodzaj dostępu, przeciągając wybrane drzwi/strefę metodą "przeciągnij i upuść" na odpowiednie pole.

Użytkownik ma do wyboru cztery rodzaje dostępów:

- Stały dostęp
- Dostęp okresowy
- Dostęp tymczasowy
- Dostęp indywidualny

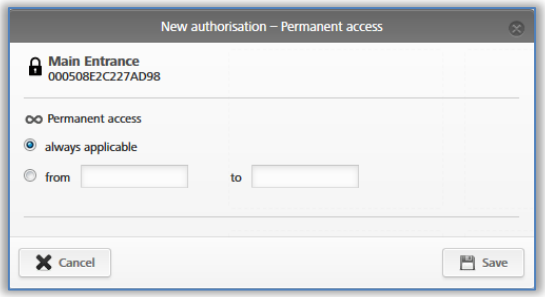
4.14.1 Stały dostęp

Stały dostęp oznacza, że dostęp jest możliwy przez całą dobę. Ograniczenie uprawnienia można zdefiniować poprzez skonfigurowanie daty początkowej i końcowej.



Rys. 77: Przyznawanie uprawnień dostępu stałego

> Ustalić okres stałego dostępu.
Można wybrać między nieograniczonym stałym dostępem i stałym dostępem z określoną datą początkową i końcową.

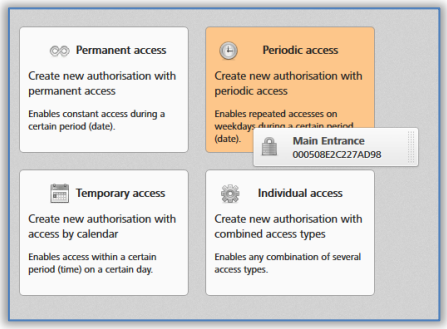


Rys. 78: Przyznawanie uprawnień dostępu stałego

> Kliknąć przycisk ***Zapisz***.

4.14.2 Dostęp okresowy

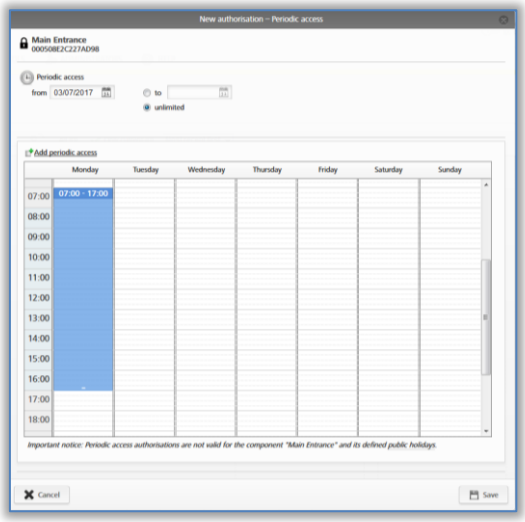
Przyznanie uprawnień do dostępu okresowego następuje w przypadku powracających dostępów w zdefiniowanym okresie. Ten powracający dostęp można porównać z seryjnym terminem, obowiązującym w cyklu tygodniowym.



Rys. 79: Przyznawanie dostępu okresowego

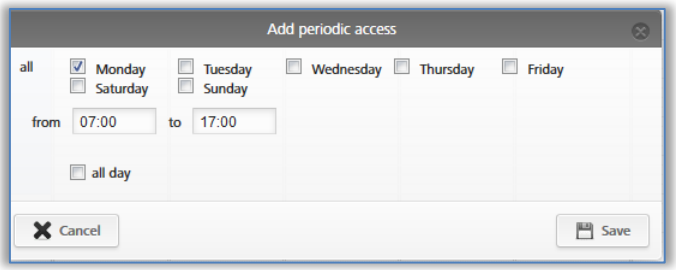
Zostanie wyświetlony widok kalendarza tygodniowego, w którym można zdefiniować maks. do 4 zakresów czasowych dla każdego dnia tygodnia.

> Ustalić okres dla dostępów czasowych.



Rys. 80: Przyznawanie dostępu okresowego

> Okres należy zdefiniować, zaznaczając go bezpośrednio w kalendarzu lub za pomocą opcji ***Dodaj okresowy dostęp***.



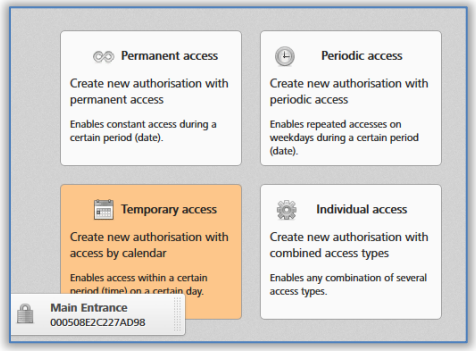
Rys. 81: Dodawanie dostępu okresowego

> Wprowadzić żądany okres i kliknąć przycisk ***Zapisz***.

> W oknie "Nowe uprawnienie – okresowy dostęp" kliknąć przycisk ***Zapisz***.

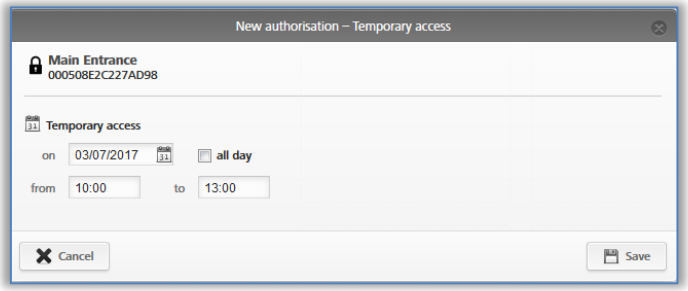
4.14.3 Dostęp tymczasowy

Uprawnienie dostępu jednorazowego należy przyznawać, jeśli będzie ono obowiązywać tylko w danym dniu, w trakcie zdefiniowanego okresu.



Rys. 82: Przyznawanie dostępu tymczasowego

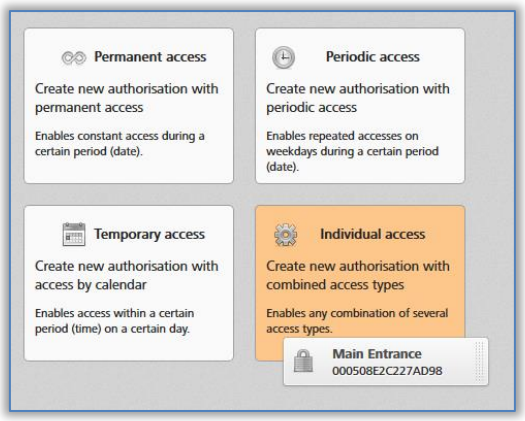
> Wprowadzić żądany okres i kliknąć przycisk ***Zapisz***.



Rys. 83: Przyznawanie dostępu tymczasowego

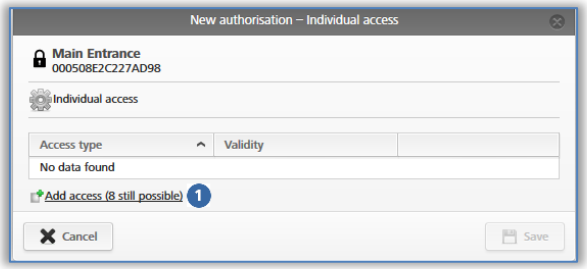
4.14.4 Dostęp indywidualny

Uprawnienie dostępu indywidualnego należy przyznawać, jeśli zachodzi potrzeba zastosowania kombinacji dostępu stałego, jednorazowego i okresowego.



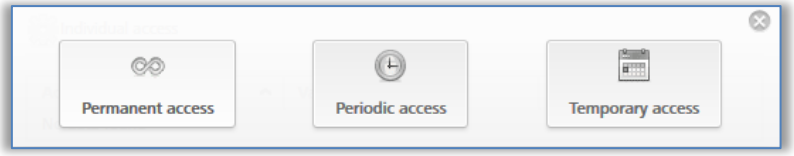
Rys. 84: Przyznawanie dostępu indywidualnego

- W oknie dialogowym "Nowe uprawnienie – dostęp indywidualny" zostaną wyświetlone już przyznane dostępy indywidualne.
- Kliknąć wartość wpisaną w wierszu, aby zmienić uprawnienie, lub
- Kliknąć opcję ***Dodaj dostęp*** ❶, aby wprowadzić nowy wpis.



Rys. 85: Nowe uprawnienie – dostęp indywidualny

- Wybrać ***stały dostęp***, ***dostęp okresowy*** lub ***dostęp tymczasowy*** i odpo–wiednio je skonfigurować. Parametry odpowiadają już opisanym uprawnieniom dostępu.



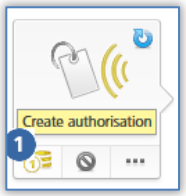
Rys. 86: Nowe uprawnienie – dostęp indywidualny

- Kliknąć przycisk ***Zapisz***, jeśli wszystkie uprawnienia dostępu indywidualnego zostały skonfigurowane.

- Stały dostęp i dostęp okresowy nie powinny się nakładać.
- Można definiować maksymalnie jeden dostęp indywidualny na dzień.
- Jeśli dostęp indywidualny i dostęp okresowy nakładają się, oba są ważne.
- Można sporządzić kombinację maksymalnie 8 indywidualnych uprawnień.

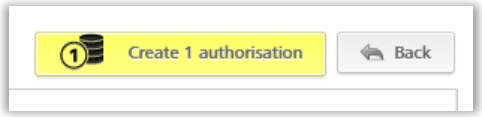
4.15 Potwierdzenie uprawnienia

Po utworzeniu uprawnień dostępu dla nośnika należy zakończyć procedurę, wybierając najpierw ***Utwórz uprawnienia***, a następnie wykonując aktualizację odpowiedniego nośnika.



Rys. 87: Utwórz uprawnienia

Poprzez zmianę istniejącego uprawnienia lub utworzenie nowego uprawnienia zmieni się symbol odpowiedniego nośnika. Jeśli użytkownik dysponuje wystarczającym kredytem, teraz można utworzyć uprawnienie.

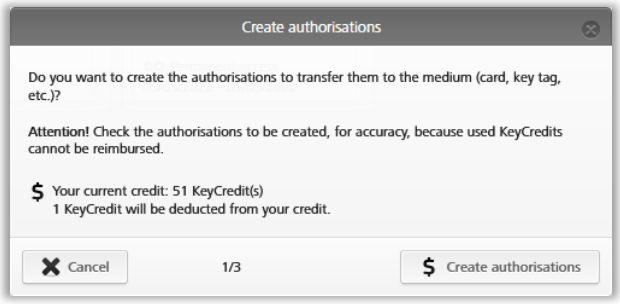


Rys. 88: Utworzenie nowego lub zmienionego uprawnienia

> Kliknąć żółty przycisk ***Utwórz 1 uprawnienie*** lub kliknąć symbol ❶ nośnika.

Jeśli użytkownik nie ma wystarczającego kredytu, aby dokonać tej czynności, pojawi się odpowiedni komunikat. Kredyt można doładować, korzystając z linku zawartego w treści tego komunikatu. Jeśli kredyt zostanie doładowany za pośrednictwem komunikatu, uprawnienie zostanie automatycznie potwierdzone i jednostka KeyCredit zostanie wyksięgowana.

> Jeśli po potwierdzeniu uprawnienia następuje wyksięgowanie kredytu ilościowego, zostanie wyświetlona odpowiednia informacja na ten temat.



Rys. 89: Utworzenie uprawnień

> Potwierdzić operację za pomocą przycisku ***Utwórz uprawnienia***.

Aby uprawnienia zadziałały na nośniku, należy za pomocą stacji kodującej lub smartfona zaktualizować nośniki (np. karty, breloki do kluczy, bransoletki lub klucze Combi). W przypadku smartfonów uprawnienia są przesyłane za pośrednictwem wiadomości typu "push".

W rozdziale dotyczącym uruchomienia przedstawiono proces początkowej konfiguracji systemu AirKey. W tematycznych podrozdziałach opisano pierwsze kroki obsługi i administracji systemu AirKey. Dokładniejszy opis poszczególnych funkcji Modułu zarządzania online systemu AirKey i aplikacji AirKey można znaleźć w następnych rozdziałach.

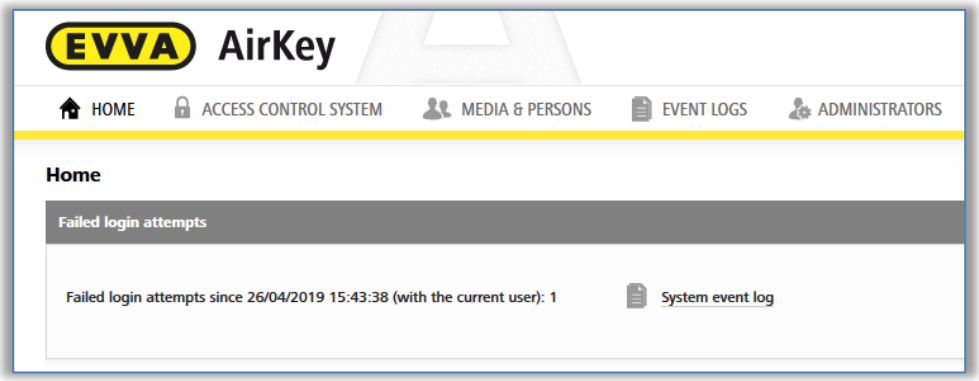
5 Moduł zarządzania online systemu AirKey

5.1 Logowanie do systemu AirKey

Logowanie jest konieczne, aby skonfigurować system zamknięć AirKey lub nim zarządzać. W ustawieniach Modułu zarządzania online systemu AirKey opcjonalnie można uaktywnić uwierzytelnienie dwuetapowe. Uaktywnienie jest opisane w rozdziale Ustawienia systemu zamknięć AirKey.

Uaktywnij uwierzytelnienie dwuetapowe, aby zwiększyć bezpieczeństwo swojego systemu zamknięć AirKey.

Nieudane próby logowania są wyświetlane na stronie startowej i protokołowane w protokole systemowym. Wskaźnik na stronie startowej ukazuje się tylko, jeżeli po ostatnim udanym logowaniu miała miejsce co najmniej jedna nieudana próba logowania.

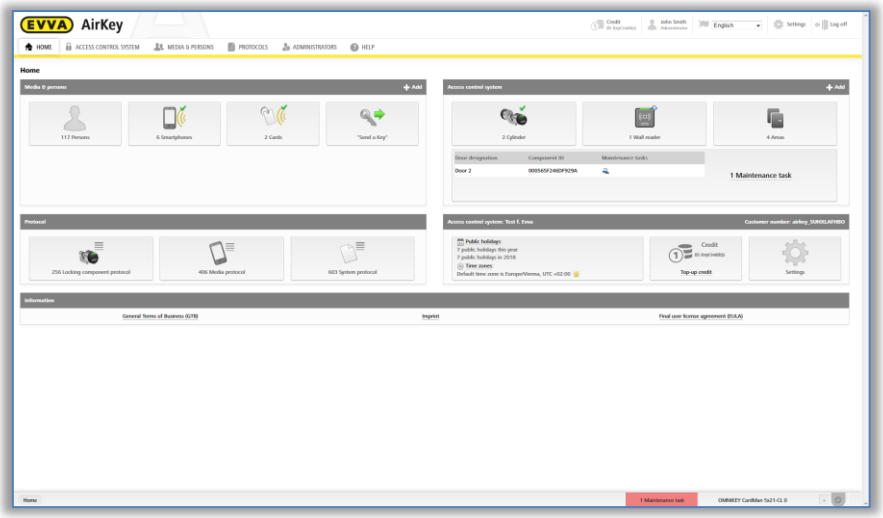


Rys. 90: Nieudane próby logowania

5.1.1 Logowanie w systemie AirKey bez uwierzytelnienia dwuetapowego

- Otworzyć w przeglądarce internetowej stronę https://airkey.evva.com.
  Otworzy się strona logowania do Modułu zarządzania online systemu AirKey.
- Wprowadzić identyfikator otrzymany w wiadomości e-mail dotyczącej "Rejestracja w systemie EVVA AirKey".
- Wprowadzić hasło i potwierdzić przyciskiem ***Zaloguj się***.

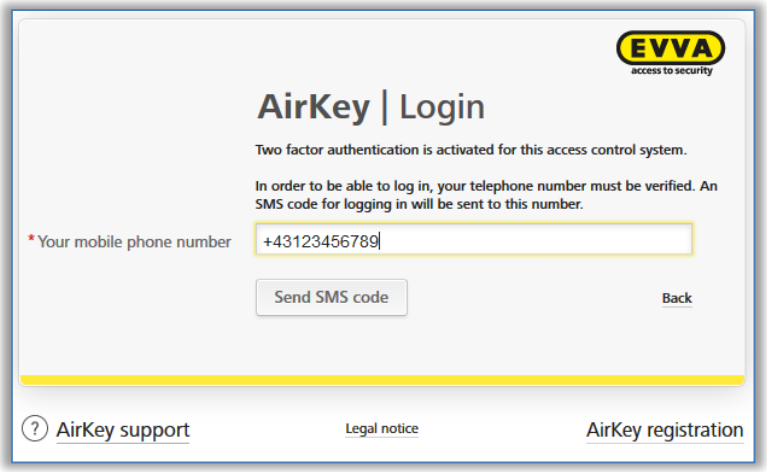
Bezpośrednio po logowaniu przejść do strony startowej ***Home***. Można tam znaleźć przegląd informacji dotyczących swojego systemu zamknięć AirKey.



Rys. 91: Moduł zarządzania online systemu AirKey – strona startowa

5.1.2 Logowanie w systemie AirKey z uwierzytelnieniem dwuetapowym

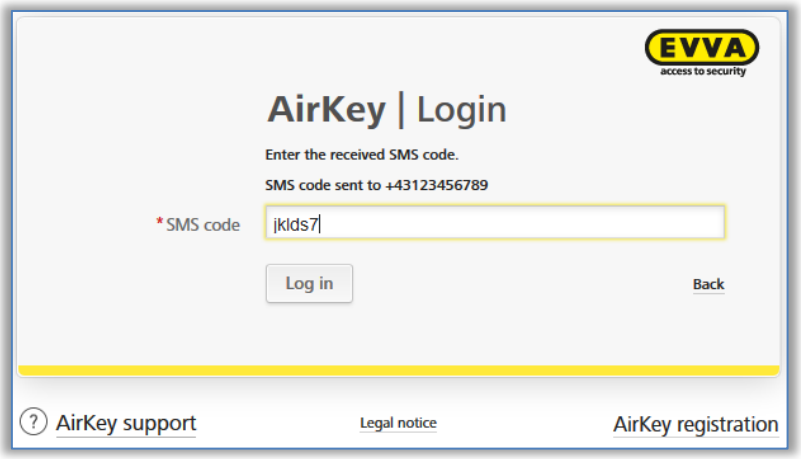
- Otworzyć w przeglądarce internetowej stronę https://airkey.evva.com.
  Otworzy się strona logowania do Modułu zarządzania online systemu AirKey.
- Wprowadzić identyfikator otrzymany w wiadomości e-mail dotyczącej "Rejestracja w systemie EVVA AirKey".
- Wprowadź wybrane hasło AirKey i potwierdź przyciskiem ***Zaloguj się***.
- Jeżeli nie został jeszcze zweryfikowany numer telefonu dla administratora, zostanie wyświetlone żądanie wpisania numeru telefonu do weryfikacji.
- Podaj numer telefoniczny smartfona, który ma być wykorzystany do uwierzytelnienia dwuetapowego, oraz potwierdź go ***Wysyłając kod SMS***. Numer telefonu musi zaczynać się od znaku **+** i numeru kierunkowego kraju, i może zawierać maksymalnie 50 znaków (+, 0-9 i spacje).



Rys. 92: Weryfikacja numerem telefonu mobilnego przy logowaniu

- Na podany numer telefonu wysyłana jest wiadomość SMS zawierająca kod SMS.

> Wpisz ten kod SMS do dialogu w module zarządzania online i potwierdź go klikając ***Zaloguj się***.



Rys. 93: Kod SMS do logowania

> W ten sposób numer telefonu został zweryfikowany przez uwierzytelnienie dwuetapowe i będzie wyświetlany na stronie startowej Twojego systemu zamknięć AirKey.

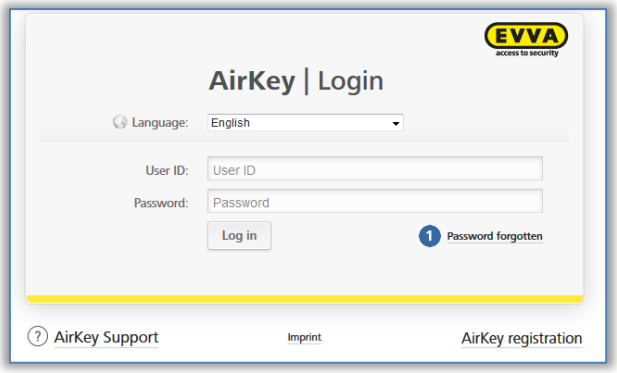
Jeżeli ten numer telefonu był już wcześniej weryfikowany, nie trzeba go ponownie wprowadzać po wprowadzeniu identyfikatora użytkownika i hasła. W takim przypadku do zweryfikowanego numeru telefonu jest od razu wysyłany kod SMS, który trzeba wpisać przy logowaniu do modułu zarządzania online.

Kod SMS jest ważny przez 5 minut. Po przekroczeniu 5 minut konieczne jest powtórzenie procedury logowania.

W razie braku dostępu do zweryfikowanego numeru telefonu można się zalogować w module zarządzania online AirKey. Aby zmienić numer telefonu, trzeba go zmienić w szczegółach administratora (patrz Edytuj administratora). Do tego celu konieczny jest jednak zweryfikowany numer telefonu. Jeżeli ten numer telefonu jest już niedostępny, zwróć się do Wsparcia technicznego EVVA.

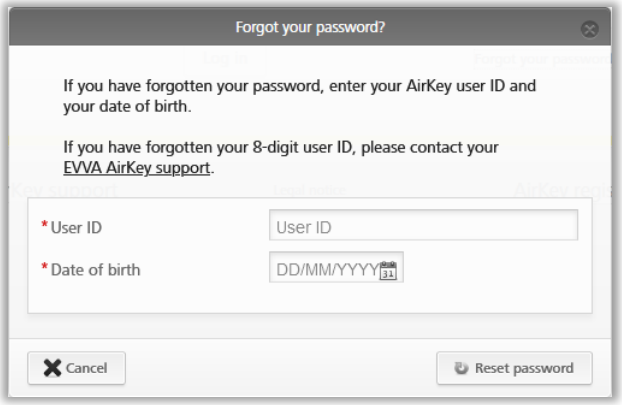
5.1.3 Utracone hasło

Jeśli użytkownik nie pamięta hasła, istnieje możliwość samodzielnego zresetowania hasła. Kliknąć przycisk ***Zapomniałeś hasło*** ❶.



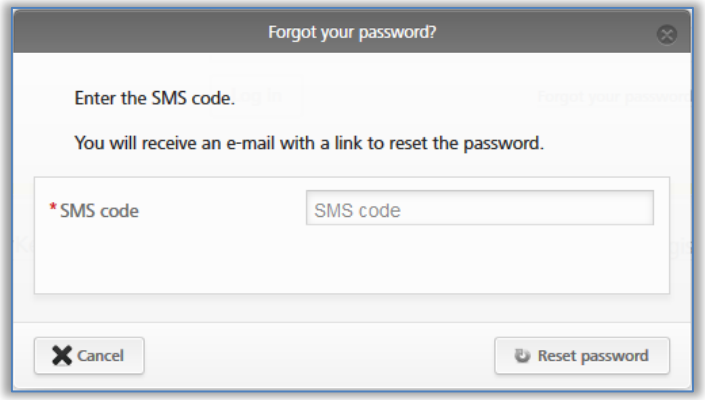
Rys. 94: Strona logowania do modułu zarządzania online AirKey

> W oknie dialogowym "Nie pamiętasz hasła?" wprowadzić swój identyfikator oraz datę urodzenia podaną podczas rejestracji, a następnie kliknąć przycisk ***Zresetuj hasło***.



Rys. 95: Utracone hasło

> Przy aktywnym uwierzytelnieniu dwuetapowym otrzymasz kod SMS w swoim zweryfikowanym smartfonie, który musi być wprowadzony w poniższym dialogu i potwierdzony funkcją ***Zresetuj hasło***. (Ta operacja nie występuje, gdy uwierzytelnienie dwuetapowe nie jest uaktywnione lub numer telefonu nie został zweryfikowany.)



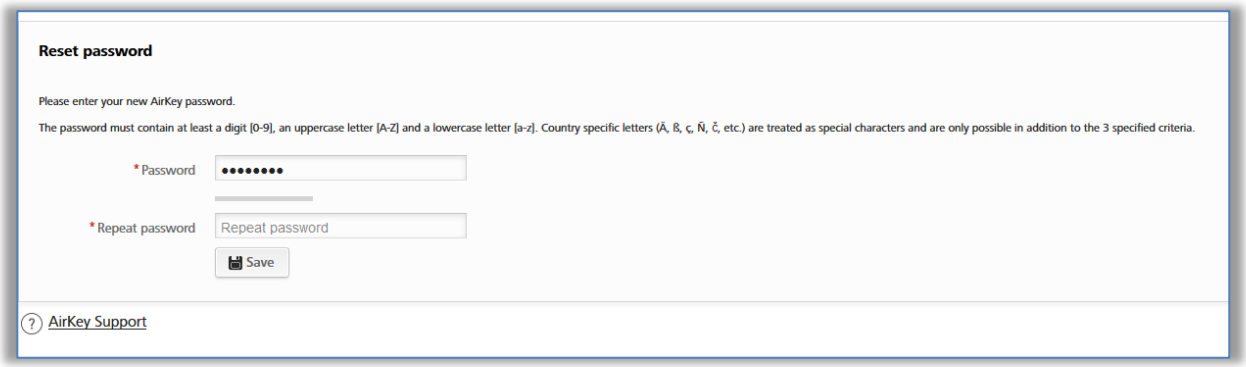
Rys 96: Kod SMS Zresetuj hasło

Kod SMS jest ważny przez 5 minut. Po przekroczeniu 5 minut procedura musi być powtórzona.

Bez dostępu do zweryfikowanego numeru telefonu nie można zakończyć procedury. Jeżeli ten numer telefonu jest już niedostępny, zwróć się do Wsparcia technicznego EVVA.

Użytkownik otrzyma automatycznie wygenerowaną wiadomość e-mail od firmy EVVA, o temacie "Reset hasła w systemie AirKey firmy EVVA".

- Otworzyć wiadomość e-mail od firmy EVVA, dotyczącą systemu AirKey.
- Kliknąć link zawarty w treści wiadomości, aby wykonać reset hasła. Otworzy się strona internetowa "Resetowanie hasła".
- Wprowadzić dwukrotnie nowe hasło.
- Kliknąć przycisk ***Zapisz hasło***.



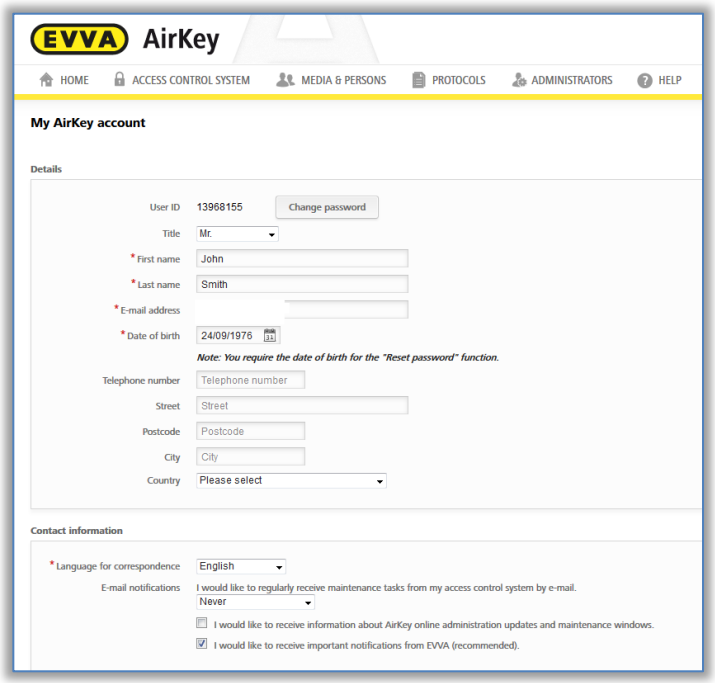
Rys. 97: Resetowanie hasła AirKey

Nastąpi przejście do strony logowania Modułu zarządzania online systemu AirKey.

- Wykonaj logowanie jak w opisie Logowanie AirKey bez uwierzytelnienia dwuetapowego albo Logowanie w systemie AirKey z uwierzytelnieniem dwuetapowym, używając nowego hasła.

Jeśli wprowadzone dane są prawidłowe, otworzy się strona startowa ***Home*** Modułu zarządzania online systemu AirKey. Z prawej strony, na górze okna wyświetlana jest nazwa zalogowanego użytkownika.

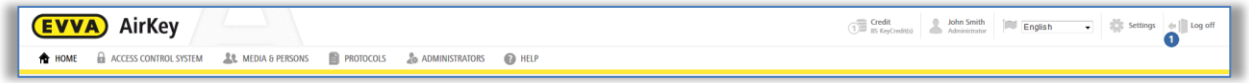
W razie potrzeby można zmienić swoje hasło także w Module zarządzania online systemu AirKey. W tym celu w prawym wierszu nagłówka modułu zarządzania online kliknąć nazwę administratora i użyć funkcji ***Zmień hasło***.



Rys. 98: Moje konto AirKey

5.2 Wylogowanie z systemu AirKey

Aby zakończyć pracę z Modułem zarządzania online systemu AirKey, należy kliknąć opcję ***Wyloguj się*** ❶.



Rys. 99: Wylogowanie

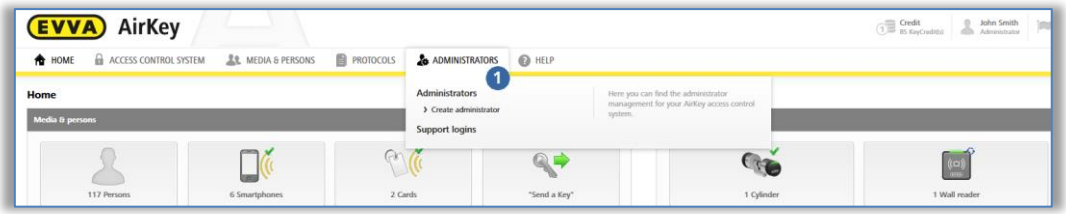
Pomimo automatycznego wylogowania po upływie 30 minut, zdecydowanie zaleca się, aby administrator po zakończeniu pracy w Module zarządzania online systemu AirKey zawsze wychodził z systemu za pomocą funkcji ***Wyloguj się***.

5.3 Administratorzy

Administratorzy dysponują wszystkimi uprawnieniami do zarządzania całym systemem zamknięć AirKey.

Należy utworzyć co najmniej jednego administratora dla danego klienta i systemu zamknięć.

Funkcje zarządcze administratora można znaleźć w menu głównym ***Administratorzy*** ❶.

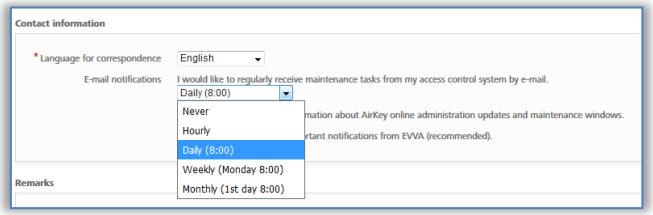


Rys. 100: Menu główne – Administratorzy

5.3.1 Utworzenie administratora

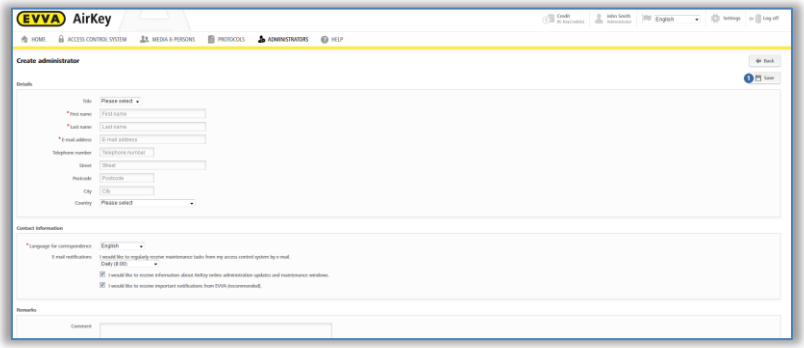
Nowi administratorzy mogą być utworzeni wyłącznie przez innych administratorów.

- Wybrać w menu głównym opcje ***Administratorzy → Utwórz administratora***.
- Wypełnić pola formularza. Pola oznaczone gwiazdką (*) są obowiązkowe.
- W bloku "Informacje kontaktowe", możesz jeszcze podać, czy administrator ma otrzymywać powiadomienia e-mail o określonych zdarzeniach, np. otwartych zadaniach konserwacyjnych, nadchodzących okresach konserwacji lub innych ważnych informacjach. Powiadomienia e-mail są wysyłane w języku wybranym do korespondencji.



Rys. 101: Informacje do kontaktu

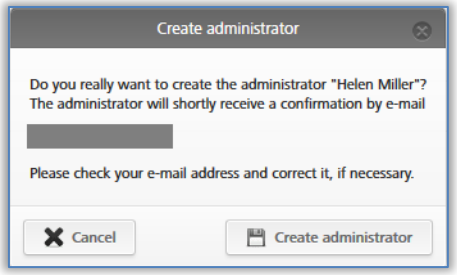
- Kliknąć przycisk ***Zapisz*** ❶.



Rys. 102: Utworzenie administratora

Przed zapisaniem danych należy ponownie sprawdzić poprawność adresu e-mail, na który po potwierdzeniu zostanie wysłany link aktywacyjny.

> Aby zakończyć operację, należy potwierdzić pytanie bezpieczeństwa, klikając przycisk ***Utwórz administratora***.



Rys. 103: Utworzenie administratora

Pomyślne utworzenie administratora będzie potwierdzone komunikatem "Administrator został zapisany".

Utworzony administrator otrzyma teraz od firmy EVVA wiadomość e-mail, zawierającą link aktywacyjny.

Jeśli link aktywacyjny nie zostanie uruchomiony w ciągu 48 godzin, dane zostaną skasowane i link aktywacyjny utraci ważność.

Utworzony administrator musi zakończyć swoją rejestrację w następujący sposób:

> Otworzyć e-mail z tematem "Rejestracja w systemie EVVA AirKey".
> Kliknąć link aktywacyjny. Otworzy się strona internetowa "Witamy w systemie AirKey".
> Wprowadzić dwukrotnie wybrane hasło oraz datę urodzenia.
> Kliknąć przycisk ***Zapisz***.

W ten sposób operacja utworzenia administratora zostanie zakończona. Teraz nastąpi przełączenie do strony logowania do Modułu zarządzania online systemu AirKey, na której nowy administrator może zalogować się.

5.3.2 Edycja administratora

Istnieje możliwość edytowania danych (np. nazwisko, adres e-mail lub numer telefonu) lub danych do kontaktu wybranego administratora w późniejszym okresie.

Nie ma możliwości zmiany identyfikatora.

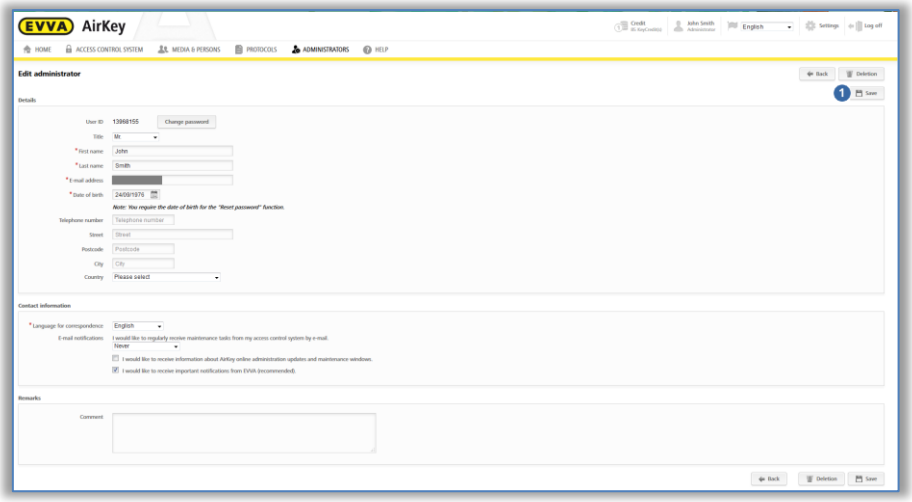
> Wybrać w menu głównym opcje ***Administratorzy*** → ***Administratorzy***.
Zostanie wyświetlona lista wszystkich aktywnych administratorów.

W ramach wyświetlonej listy użytkownik może wyszukać danego administratora, sortować kolumny, ograniczyć liczbę wyświetlanych wpisów na stronę lub wyeksportować listę do pliku CSV.

> Kliknąć pozycję administratora, którego dane mają być zmienione.

> Zmienić żądane dane.

> Kliknąć przycisk ***Zapisz*** ❶.



Rys. 104: Edycja administratora

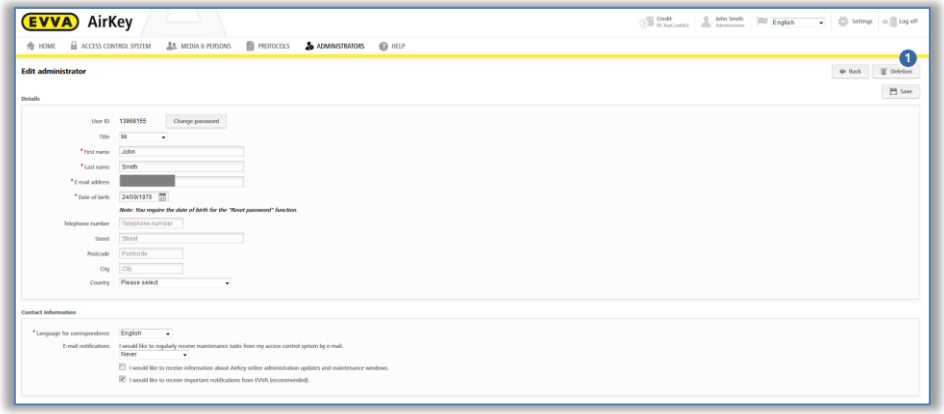
5.3.3 Kasowanie administratora

Administrator może zostać usunięty z systemu tylko przez innego administratora.

> Kliknąć w menu głównym opcje ***Administratorzy*** → ***Administratorzy***.

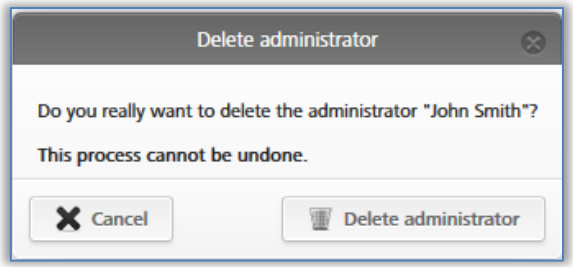
> Wybrać administratora, który ma zostać skasowany, poprzez kliknięcie odpowiedniego wiersza w tabeli. Nastąpi przejście do strony "Edycja administratora".

> Kliknąć przycisk ***Usuń*** ❶.



Rys. 105: Kasowanie administratora

> Potwierdzić pytanie bezpieczeństwa przyciskiem ***Skasuj administratora***.



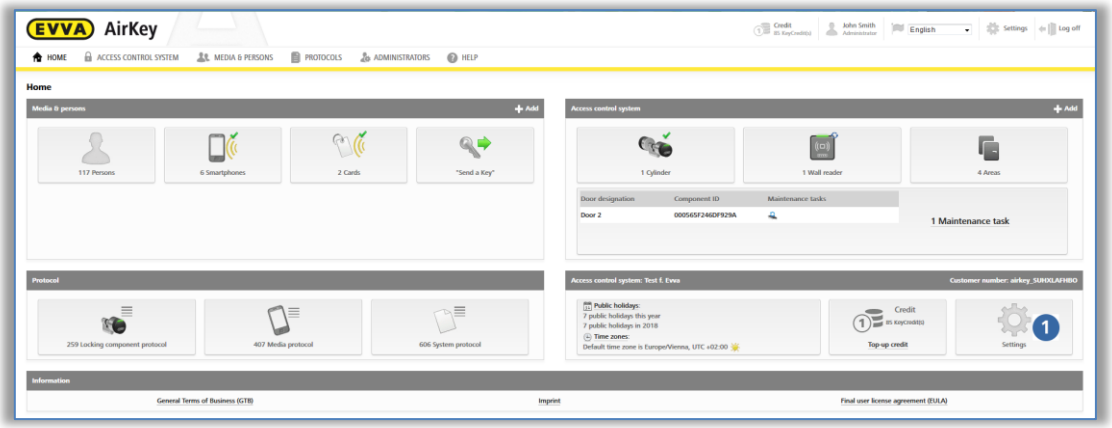
Rys. 106: Kasowanie administratora

Pomyślne skasowanie administratora będzie potwierdzone komunikatem "Administrator został usunięty". Skasowany administrator nie będzie już wyświetlany na liście administratorów i nie będzie mógł zalogować się do Modułu zarządzania online systemu AirKey.

5.4 Ustawienia systemu AirKey

W ustawieniach Modułu zarządzania online systemu AirKey odbywa się konfiguracja podstawowych ustawień, które dokładniej opisano w dalszej części podręcznika.

- Na stronie startowej ***Home*** wybrać ikonę ***Ustawienia*** ❶.
- Alternatywnie w wierszu nagłówka kliknąć opcję ***Ustawienia***.



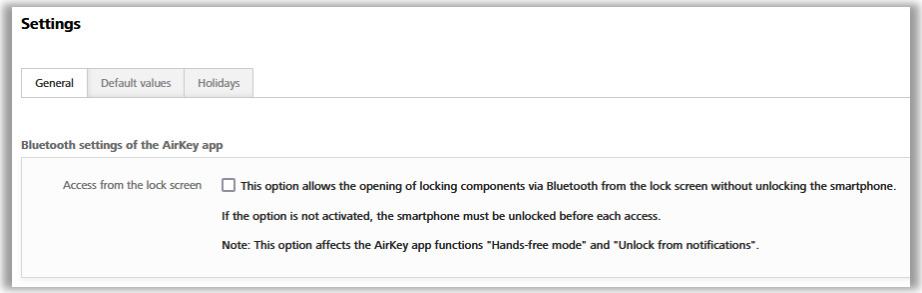
Rys. 107: Ustawienia systemu AirKey

5.4.1 Informacje ogólne

Na tej zakładce można uaktywnić poniższe ogólne ustawienia dla całewgo systemu zamknięć.

Ustawienia Bluetooth dla aplikacji AirKey

Tutaj, dla wszystkich smartfonów w danym systemie zamknięć można skonfigurować, czy otwieranie komponentów zamykających będzie możliwe lub niemożliwe za pomocą Bluetooth z poziomu zablokowanego ekranu. Jeśli ta opcja nie jest aktywna, konieczne jest odblokowywanie smartfona przed każdym dostępem.



Rys. 108: Ogólne ustawienia – Ustawienia Bluetooth dla aplikacji AirKey

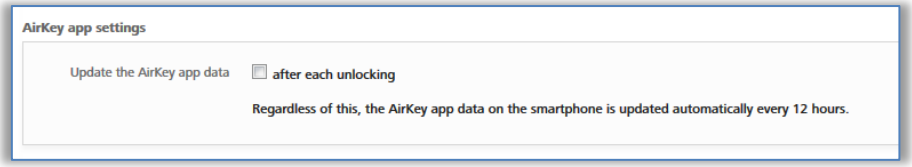
Ta opcja ma wpływ na funkcje aplikacji "Tryb Hands free" i "Odblokowanie z powiadomień".

Dezaktywuj opcję ***Dostęp z ekranu blokady***, aby zwiększyć bezpieczeństwo systemu zamknięć.

Ustawienia dla aplikacji AirKey

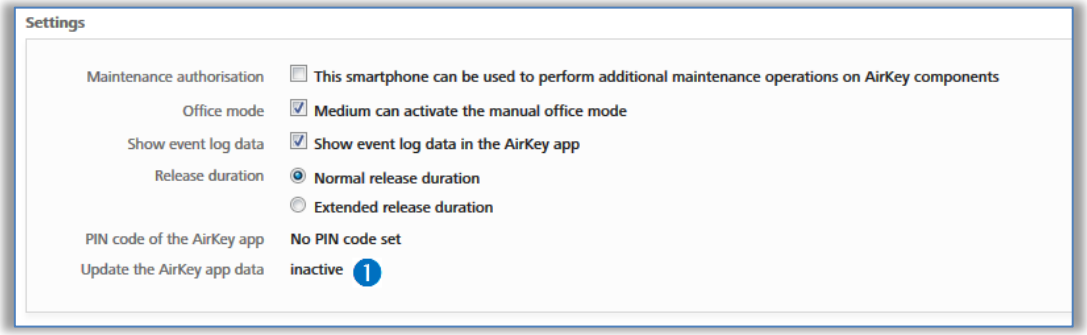
Tu można uaktywnić opcję "Aktualizacja po każdym dostępie". Jeżeli ta opcja zostanie uaktywniona, dane aplikacji AirKey (np. wpisy do protokołu lub stan baterii komponentów zamykających) będą aktualizowane przy każdym dostępie smartfonem.

> W tym celu zaznacz odpowiednią kratkę i potwierdź naciskając ***Zapisz***.



Rys. 109: Ogólne ustawienia – Ustawienia dla aplikacji AirKey

Funkcja ta zostanie rozesłana do wszystkich smartfonów danego systemu zamknięć w formie powiadomienia Push. Najpóźniej po ręcznej aktualizacji danych aplikacji AirKey smartfona (patrz rozdział Aktualizacja smartfona), funkcja powinna uaktywnić się w smartfonie. Aktualny stan ❶ smartfona w odniesieniu do tej funkcji można znaleźć w Module zarządzania online systemu AirKey w szczegółach smartfona.



Rys. 110: Stan opcji "Aktualizacja po każdym dostępie"

Uaktywnij tę funkcję, aby podczas używania smartfona dostępy były przesyłane do modułu zarządzania online praktycznie w czasie rzeczywistym.

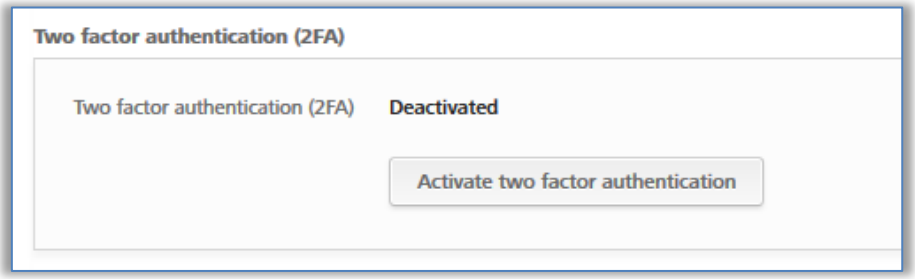
Aktualizacja danych aplikacji AirKey po każdym dostępie przesyła tylko dane tego smartfona, na którym zostało wykonane dostęp. W samym smartfonie aktualizacja na nie jest prezentowana wizualnie.

Funkcja ta wymaga stabilnego połączenia z Internetem (komórkowa transmisja danych lub WLAN), ponieważ kolejny dostęp może być wykonany dopiero po aktualizacji danych aplikacji AirKey.

Niezależnie od opcji "Aktualizacja po każdym dostępie" co 12 godzin uruchamiana jest automatycznie próba aktualizacji danych aplikacji AirKey.

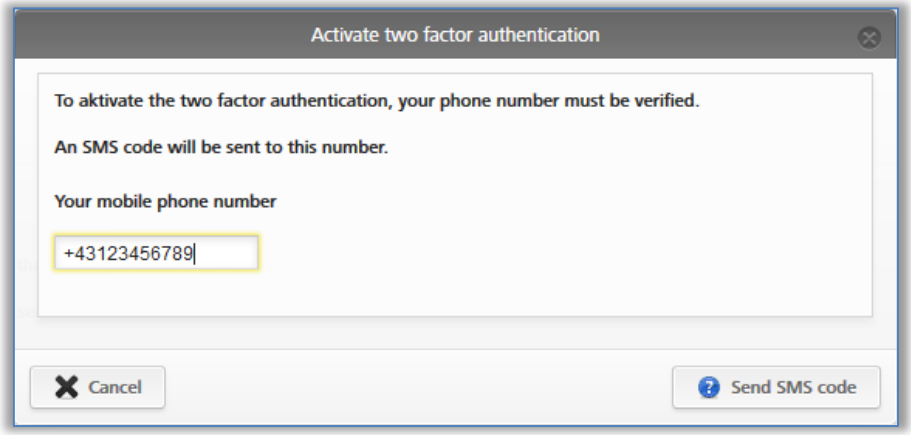
Uwierzytelnianie dwuetapowe (2FA)

- Uwierzytelnienie dwuetapowe, czyli 2FA, stanowi dodatkowy poziom zabezpieczenia przy logowaniu do Modułu zarządzania online systemu AirKey. Oprócz identyfikatora użytkownika i hasła przy logowaniu w drugim etapie sprawdzany jest dodatkowy kod SMS. Jeżeli w ustawieniach zostanie uaktywnione uwierzytelnienie dwuetapowe, jest ono wykorzystywane u wszystkich administratorów danego systemu zamknięć. W celu uaktywnienia kliknij przycisk ***Uaktywnij uwierzytelnienie dwuetapowe***.



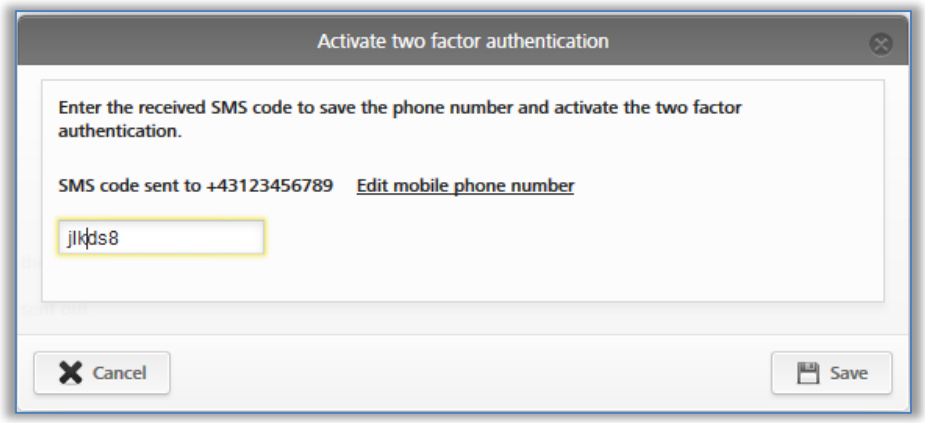
Rys. 111: Ogólne ustawienia – uwierzytelnienie dwuetapowe (2FA)

- Wpisz numer telefonu komórkowego, który ma być wykorzystywany do uwierzytelnienia dwuetapowego, dla aktualnie zalogowanego administratora i kliknij ***Wyślij kod SMS***.



Rys. 112: Wpisz numer telefonu komórkowego

- Kod SMS zostanie wysłany na podany wcześniej numer telefonu. Ten kod SMS należy wprowadzić w dialogu w module zarządzania online i potwierdzić poleceniem ***Zapisz***.



Rys. 113: Wprowadź kod SMS w ustawieniach

Jeżeli został użyty prawidłowy kod SMS, uwierzytelnienie dwuetapowe jest uaktywnione dla wszystkich administratorów systemu zamknięć. Odpowiednio zmienia się stan w ustawieniach.

Kod SMS jest ważny przez 5 minut. Po przekroczeniu 5 minut procedura musi być powtórzona.

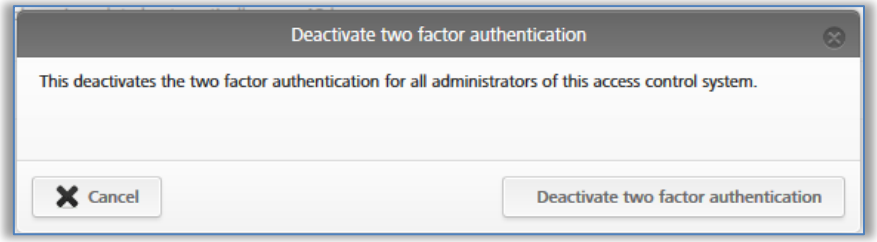
Od chwili uaktywnienia do każdego logowania niezbędny jest telefon komórkowy. Szczegóły procedury logowania z uaktywnionym uwierzytelnieniem dwuetapowym znajdziesz w rozdziale Logowanie w systemie AirKey z uwierzytelnieniem dwuetapowym.

Aby wyłączyć uwierzytelnienie dwuetapowe, wykonaj następujące operacje.

> Kliknij polecenie ***Wyłącz uwierzytelnienie dwuetapowe***.

Rys. 114: Wyłącz uwierzytelnienie dwuetapowe

> Potwierdź klikając jeszcze raz polecenie ***Wyłącz uwierzytelnienie dwuetapowe***.



Rys. 115: Wyłącz uwierzytelnienie dwuetapowe

Funkcja zostanie wyłączona dla wszystkich administratorów danego systemu zamknięć.

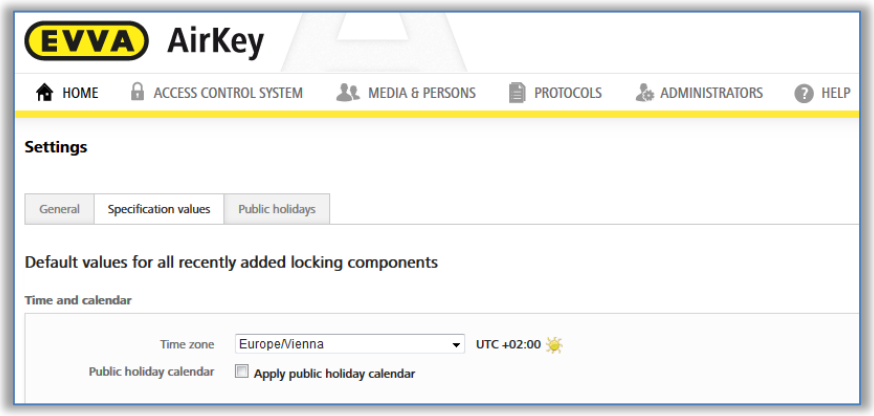
Interfejs AirKey Cloud (API)
Interfejs AirKey Cloud jest interfejsem REST (API) dla systemów zewnętrznych. Interfejs umożliwia sterowanie określonymi funkcjami AirKey za pośrednictwem oprogramowania zewnętrznego. Szczegóły na temat interfejsu AirKey Cloud są opisane w rozdziale AirKey Cloud Interface (API).

AirKey Cloud Interface (API) - środowisko testowe
Środowisko testowe umożliwia wypróbowanie interfejsu AirKey Cloud (API) przed jego uruchomieniem w środowisku zabezpieczonym z wykorzystaniem danych testowych. Szczegóły na ten temat znajdziesz w rozdziale AirKey Cloud Interface (API).

5.4.2 Wartości domyślne (dla wszystkich nowo dodanych komponentów zamykających)

Te ustawienia będą automatycznie aktywowane dla nowo dodanego komponentu zamykającego. Szczególnie w przypadku większych systemów zaleca się ustawienie wartości domyślnych przed pierwszą instalacją, aby w ten sposób uprościć administrowanie systemem.

Godzina i kalendarz
W systemie zamknięć AirKey użytkownik może zarządzać komponentami zamykającymi, które znajdują się w różnych strefach czasowych. Standardową, wstępnie przyjętą wartością domyślną jest strefa czasowa "Europa/Wiedeń" o wskazaniu UTC+01:00 porą zimową lub UTC+02:00 w miesiącach letnich, co obowiązuje na terenie Europy Środkowej.



Rys. 116: Wartości domyślne dla nowych komponentów zamykających

Jeśli użytkownik zamierza zmienić strefę czasową dla całego systemu zamknięć, wówczas należy kliknąć menu rozwijane i wybrać odpowiednią strefę.

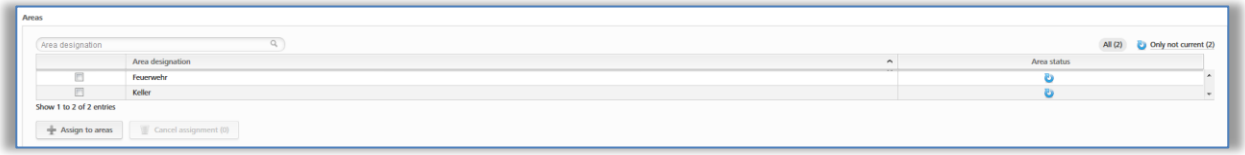
Jeśli konieczna jest zmiana strefy czasowej dla komponentu zamykającego, na stronie startowej ***Home*** kliknąć ikonę ***Wkładka*** lub ***Czytnik naścienny***, wybrać żądany komponent zamykający i przejść do zakładki ***Ustawienia***. W bloku ***Godzina i kalendarz*** także znajduje się menu rozwijane z listą stref czasowych.

Symbol słońca w przypadku danej strefy czasowej wskazuje, czy aktywny jest czas letni lub zimowy:

- Żółte słońce = czas letni
- Szare słońce = czas zimowy

Jeśli umieszczono zaznaczenie w polu ***Zastosuj kalendarz dni świątecznych***, wówczas dni świąteczne zdefiniowane i aktywowane w zakładce ***Dni świąteczne*** (patrz rozdział Dni świąteczne) zostaną zastosowane dla nowego komponentu zamykającego.

Strefy

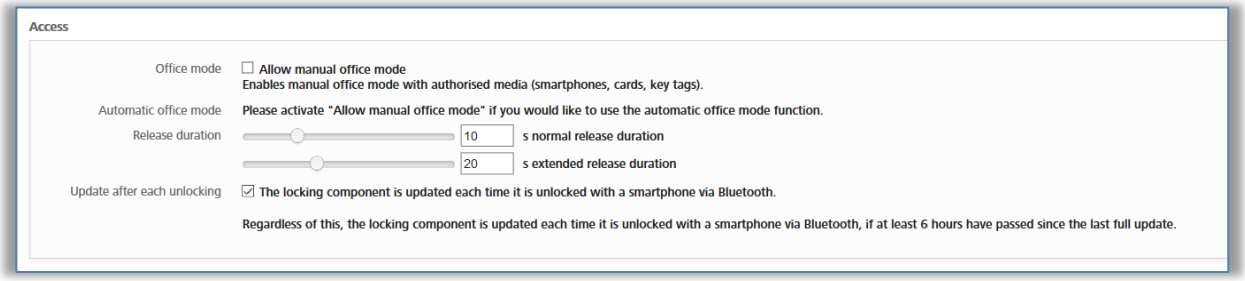


Rys. 117: Wartości domyślne – strefy

W tej sekcji można automatycznie przyporządkować nowe komponenty zamykające do już utworzonych stref. Opis utworzenia strefy został dokładniej objaśniony w rozdziale Utworzenie strefy.

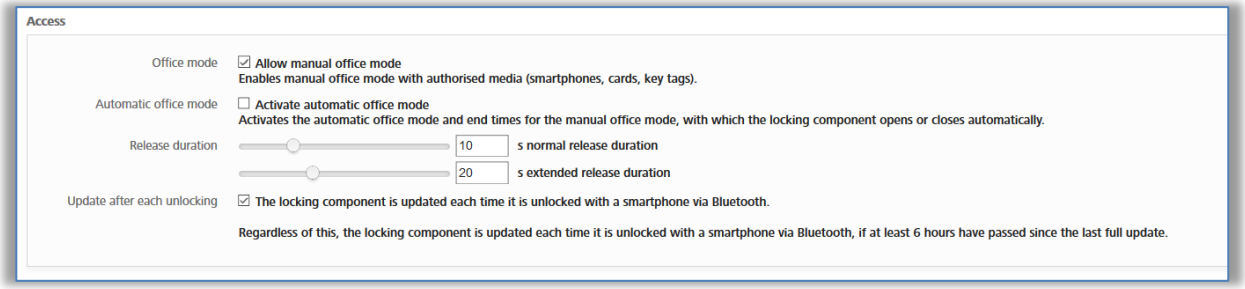
Jest to szczególnie polecane w przypadku klucza generalnego lub klucza dla straży pożarnej, które zawsze muszą odryglować wszystkie komponenty. Przyporządkowanie do stref można także anulować w przypadku wybranych komponentów zamykających.

Dostępy



Rys. 118: Wartości domyślne – dostępy

Tutaj można zezwolić na ręczne stałe otwarcie dla wszystkich nowo dodanych komponentów zamykających. Jeśli pole wyboru ***Zezwól na ręczne stałe otwarcie*** będzie aktywne, pojawi się dodatkowo kolejne pole wyboru: ***Aktywuj autom. stałe otwarcie***.

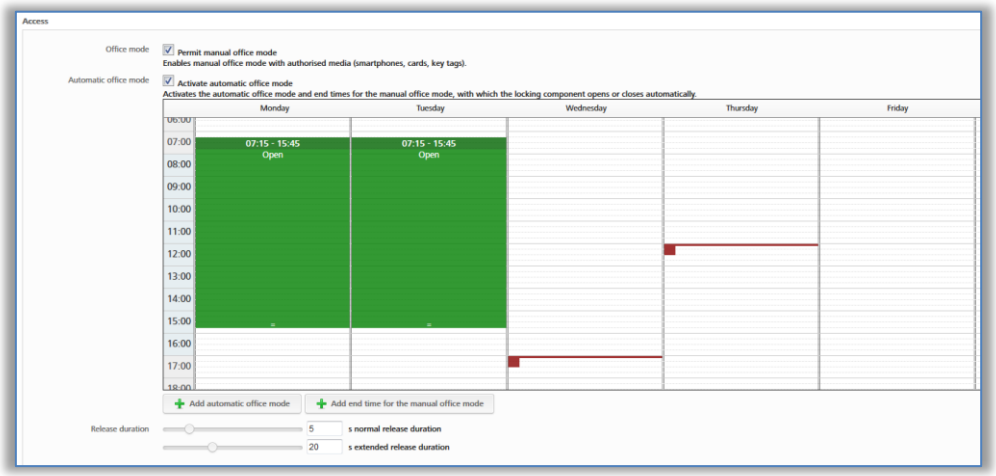


Rys. 119: Automatyczne stałe otwarcie

Automatyczne stałe otwarcie umożliwia ustawienie okresów lub momentów zamykania dla automatycznego otwierania lub zamykania komponentów. Na przykład w biurze co wieczór automatycznie kończy się stałe otwarcie o godzinie 17:00. W przypadku wkładki AirKey nie oznacza to, że drzwi zostaną zaryglowane, ale że nastąpi wysprzęglenie wkładki. Do zaryglowania drzwi wkładka musi zostać zasprzęglona za pomocą uprawnionego nośnika, a następnie ręcznie zaryglowana.

W tym oknie dialogowym można także wprowadzić czas zakończenia ręcznego stałego otwarcia. W ten sposób można zagwarantować, że niezależnie od aktywowania stałego otwarcia będzie ono w określonym momencie zakończone (czerwony pasek na dolnym zrzucie ekranu). Dla danego dnia można maksymalnie ustawić 4 pozycje (okresy lub czasy zakończenia).

Stałe otwarcia są automatycznie kończone lub w ogóle nie są rozpoczynane w dni świąteczne, w razie ostrzeżenia o rozładowanej baterii, w razie nieprawidłowej godziny w komponentach zamykających lub w razie aktualizacji firmware.



Rys. 120: Automatyczne stałe otwarcia

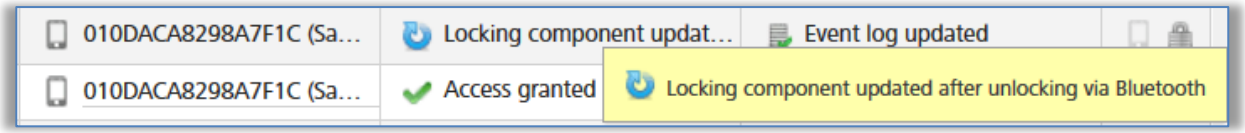
Okres zezwolenie określa, jak długo trwa zezwolenie komponentu zamykającego na użycie (np. w przypadku wkładki oznacza to, jak długo użytkownik ma możliwość ręcznego obrócenia gałki wkładki). Standardowo normalny okres zezwolenia wynosi 5 sekund, a rozszerzony – 20 sekund. Okres zezwolenie można tutaj indywidualnie dopasować w zakresie od 1 sekundy do 250 sekund.

Ręczne stałe otwarcie można także aktywować za pomocą nośników dostępu. Wówczas nośnik należy przytrzymać przy komponencie zamykającym, na krótko usunąć z obszaru odczytywania i drugi raz przyłożyć nośnik w trakcie okresu otwarcia. W ten sposób można także zakończyć ręczne stałe otwarcie.

Za pomocą opcji ***Aktualizacja po każdym odblokowaniu*** można zdecydować, czy komponent zamykający ma zostać zaktualizowany po każdej pomyślnej operacji odryglowania Bluetooth. Niezależnie od tego komponent blokujący jest aktualizowany za każdym razem, kiedy zostanie zaryglowany przez smartfon poprzez Bluetooth i jeśli od ostatniej pełnej aktualizacji minęło co najmniej 6 godzin.

Ta aktualizacja będzie niezauważalna dla użytkownika. Nie będzie ona sygnalizowana ani nie spowoduje wyświetlenia informacji na smartfonie.

Jednak administrator zobaczy tę czynność w protokołach w Module zarządzania online systemu AirKey.



Rys. 121: Protokołowanie – Aktualizacja po operacji odryglowania

Podczas aktualizacji po operacji odryglowania Bluetooth aktualizowane są wyłącznie następujące dane:

- Czarna lista
- Strefa czasowa
- Godzina
- Wpisy do protokołu

Gdy komponent zamykający ma jeszcze inne otwarte zadania konserwacyjne, należy je zaktualizować zgodnie z opisem w rozdziale Aktualizowanie komponentów zamykających.

Funkcja jest zależna od jakości połączenia smartfona. Dlatego należy pamiętać o zapewnieniu stabilnego połączenia z Internet w ramach sieci 3G (lub lepszej) lub przez WLAN.

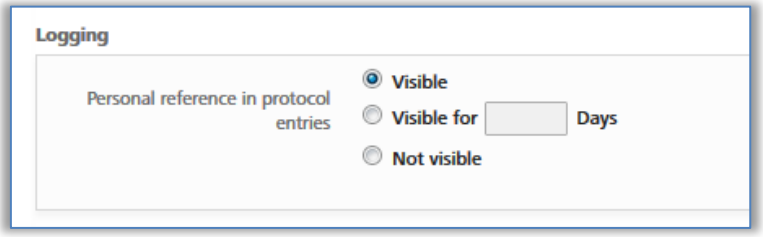
Aktualizacja po operacji odryglowania Bluetooth będzie również przeprowadzana po uruchomieniu ręcznego stałego otwarcia, ale nie w momencie jego zakończenia.

Aktualizacja po operacji odryglowania Bluetooth następuje w okresie zezwolenia komponentu zamykającego. W przypadku okresu zezwolenia poniżej 10 sekund aktualizacja po operacji odryglowania Bluetooth może nie funkcjonować. Dlatego podczas aktywowania funkcji następuje automatyczne zwiększenie wartości normalnego okresu zezwolenia do 10 sekund.

Aktywowanie tej funkcji zwiększa zużycie baterii w komponentach zamykających zasilanych bateryjnie, takich jak np. wkładka AirKey, a także wpływa na żywotność baterii.

Protokołowanie

Wybrać wartość domyślną dla protokołowania odniesień osobowych podczas zdarzeń dostępu. Użytkownik ma tu trzy opcje do wyboru:



Rys. 122: Konfiguracja protokołowania

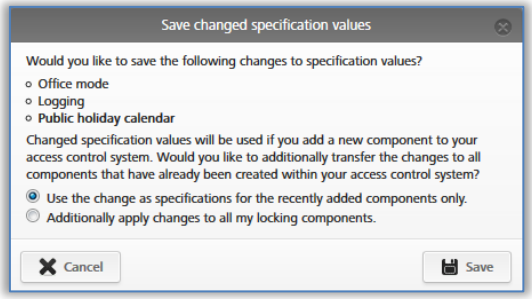
Widoczne pozwala na wyświetlanie danych osobowych ze zdarzeń dostępowych bez ograniczenia czasowego.

Widoczne przez ... dni spowoduje anonimizację danych osobowych ze zdarzeń dostępowych po określonej liczbie dni.

Niewidoczne spowoduje anonimizację wszystkich danych osobowych ze zdarzeń dostępowych.

Zdefiniowane wartości domyślne można zmienić dla poszczególnych elementów zamykających, niezależnie od przyjętych tutaj ustawień.

Zmienione wartości domyślne należy zapisać, naciskając przycisk ***Zapisz***. W tym celu pojawi się pytanie, czy zmienione wartości domyślne mają być stosowane w przypadku nowo dodanych lub wszystkich komponentów zamykających.



Rys. 123: Zapisanie zmienionych wartości domyślnych

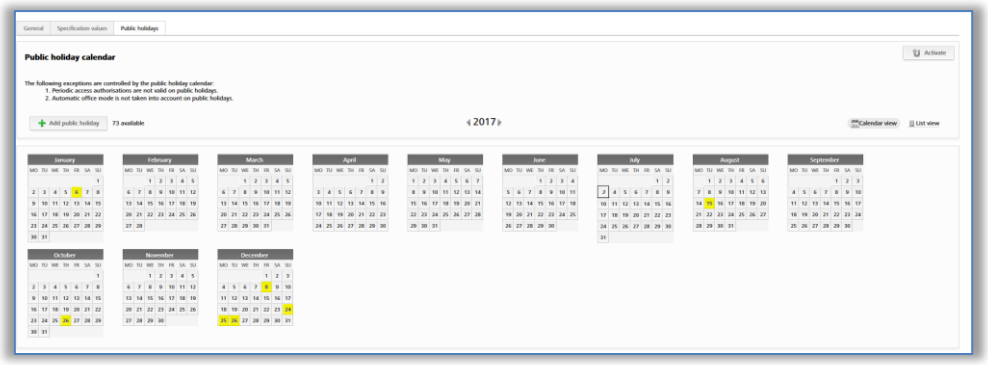
5.4.3 Dni świąteczne

W zakładce ***Dni świąteczne*** można zdefiniować maksymalnie 80 dni świątecznych na rok (aktualny rok i dwa lata kolejne). Pojęcie "dnia świątecznego" w systemie AirKey może oznaczać ustawowo wolny dzień od pracy, ale także kilkudniowy okres, np. przerwę urlopową lub ferie szkolne, które mogą się powtarzać. Na przykład święta krajowe lub dni świąteczne, które co roku mają tę samą datę, można określić jako powtarzalne co roku. Tydzień ferii szkolnych oznacza tylko 1 dzień świąteczny, gdy zostanie zdefiniowany jako okres z wartościami początek–koniec.

Oddziaływanie kalendarza dni świątecznych:

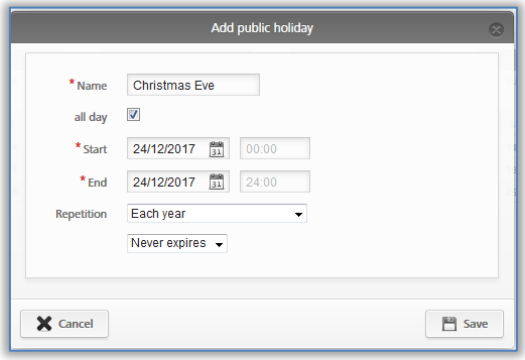
1. Okresowe uprawnienia dostępu nie są ważne w dniach świątecznych.
2. Automatyczne stałe otwarcia nie są uwzględniane w dniach świątecznych.

Aby kalendarz dni świątecznych obowiązywał, należy go aktywować globalnie przyciskiem ***Aktywuj*** z prawej strony ekranu.



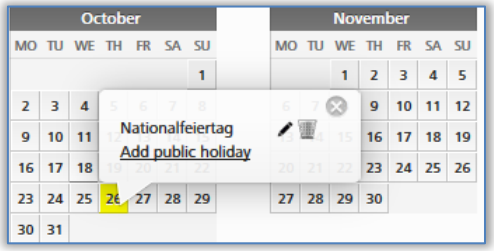
Rys. 124: Kalendarz dni świątecznych (widok kalendarza)

Kliknąć przycisk ***Dodaj dzień świąteczny*** lub w widoku kalendarza kliknąć dokładną datę dnia świątecznego (np. 24.12), wówczas otworzy się okno dialogowe, w którym można wprowadzić nazwę dnia świątecznego, czy dzień świąteczny obowiązuje przez cały dzień, od kiedy do kiedy trwa dzień świąteczny (np. tylko po południu – można tu także zdefiniować np. przerwy wakacyjne), jak często powtarza się dany dzień świąteczny i kiedy kończy się powtarzalność.



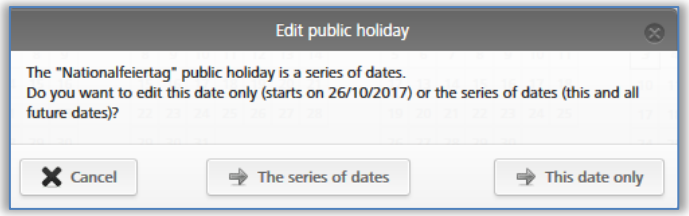
Rys. 125: Dodawanie dnia świątecznego

Każdy już wprowadzony dzień świąteczny można później edytować; w tym celu należy kliknąć wybrany dzień – otworzy się okno tekstowe.

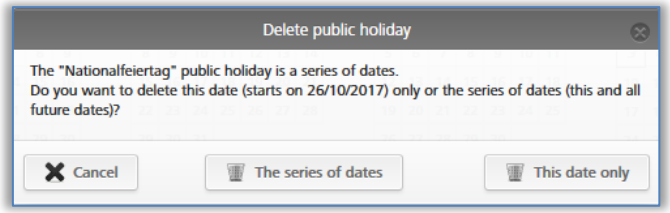


Rys. 126: Dodawanie dnia świątecznego poprzez kalendarz

Klikając link ***Dodaj dzień świąteczny***, można dodać kolejny dzień świąteczny w tym dniu. Dla jednego dnia kalendarzowego można wprowadzić kilka dni świątecznych. Kliknięcie symbolu ołówka umożliwia edytowanie dnia świątecznego, kliknięcie symbolu kosza umożliwi usunięcie dnia świątecznego.

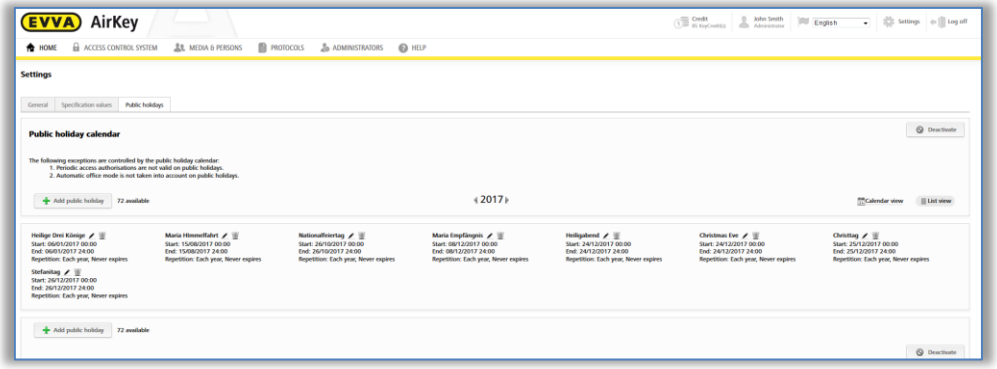


Rys. 127: Edycja dnia świątecznego



Rys. 128: Usuwanie dnia świątecznego

Po wprowadzeniu terminów, przerw wakacyjnych / urlopów lub dni świątecznych do kalendarza przegląd wszystkich zapisanych dni świątecznych itp. zostanie wyświetlony w formie listy.

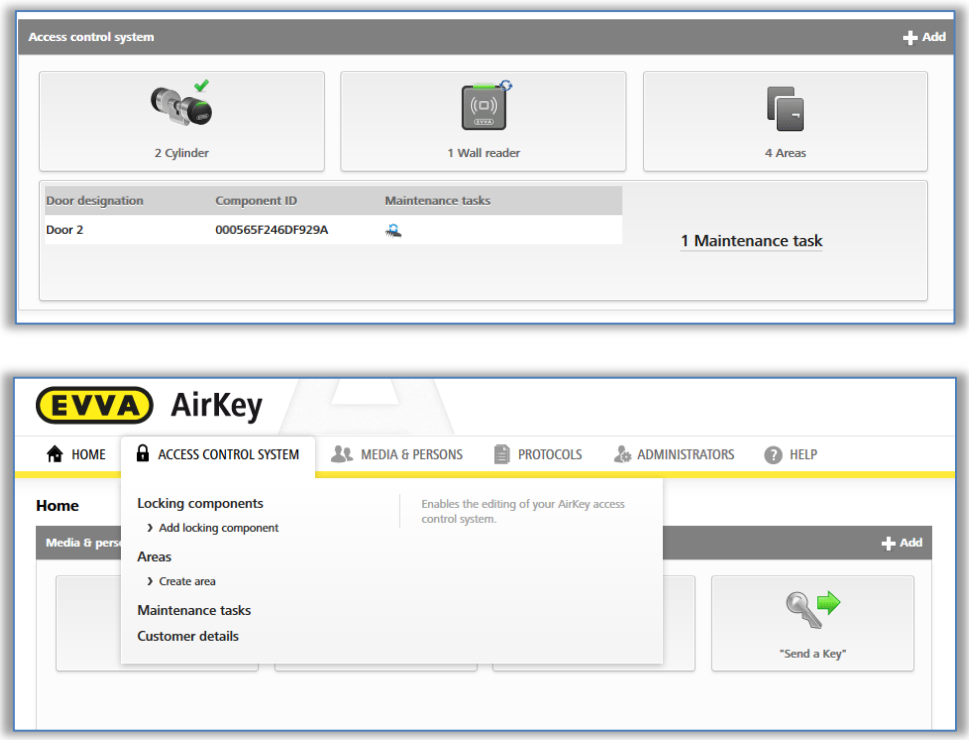


Rys. 129: Kalendarz dni świątecznych (widok listy)

Po wybraniu przycisku ***Dezaktywuj*** nastąpi globalna dezaktywacja kalendarza dni świątecznych dla systemu zamknięć, który nie będzie zastosowany wobec dodanych komponentów zamykających.

5.5 System zamknięć

Ikony na stronie startowej ***Home*** lub punkty menu i podmenu w menu głównym ***System zamknięć*** służą do zarządzania systemem AirKey.

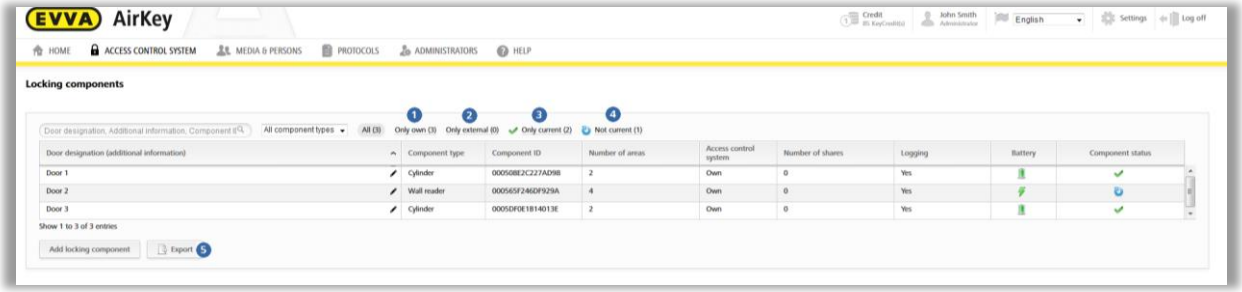


Rys. 130: System zamknięć AirKey

5.5.1 Przegląd komponentów zamykających

Aby wyświetlić przegląd wszystkich komponentów zamykających systemu AirKey, na stronie startowej ***Home*** należy kliknąć ikonę ***Wkładka*** lub ***Czytnik naścienny***, lub w menu głównym ***System zamknięć*** → ***Elementy zamykające***. Na stronie startowej ***Home*** pojawi się wskazanie liczby wkładek lub czytników naściennych zintegrowanych w systemie zamknięć.

Zostanie wyświetlona lista wszystkich komponentów zamykających wraz z ich statusem, a także informacje dodatkowe. W pierwszym wierszu listy, obok pola wyszukiwania, znajdują się także funkcje filtrowania komponentów zamykających.



Rys. 131: Komponenty zamykające

- "Tylko własne" ❶ to filtr, który spowoduje wyświetlenie tylko własnych komponentów zamykających.
- "Tylko nieznane" ❷ to filtr, który spowoduje wyświetlenie wyłącznie komponentów zamykających udostępnionych przez administratora.

- "Tylko aktualne" ❸ to filtr, który spowoduje wyświetlenie tylko komponentów zamykających z aktualnym statusem.
- "Nieaktualne" ❹ to filtr, który spowoduje wyświetlenie tylko komponentów zamykających bez aktualnego statusu.
- Listę komponentów zamykających można eksportować do pliku CSV w celu dalszego przetwarzania ❺.

System AirKey umożliwia udostępnienie komponentów zamykających obcemu systemowi zamknięć AirKey. Na liście uwzględniono rozróżnienie pomiędzy własnymi i obcymi komponentami zamykającymi. Bliższe informacje na temat można znaleźć w rozdziale Udostępnianie komponentów zamykających dla innych systemów zamknięć.

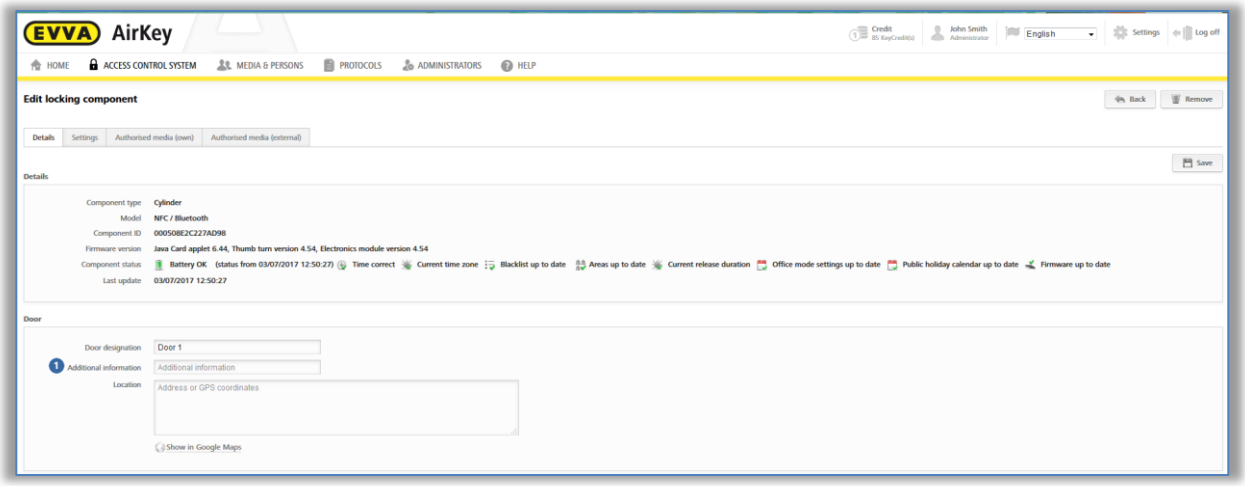
5.5.2 Dodawanie komponentu zamykającego: patrz rozdział 4.11

5.5.3 Edycja komponentu zamykającego

W oknie ***Edytuj komponent zamykający***, w zakładce ***Szczegóły*** znajdują się różne informacje, takie jak np. typ i model komponentu, ID komponentu, wersja oprogramowania firmware lub status komponentu, a także informacje dotyczące drzwi, stref i udostępnień. Dodatkowo można tutaj wyświetlić lokalizację komponentu zamykającego na stronie Google Maps. W zakładce ***Ustawienia*** można przejrzeć wszystkie zdefiniowane ustawienia dotyczące strefy czasowej i kalendarza dni świątecznych, a także dostępu, protokołowania i opcji naprawy.

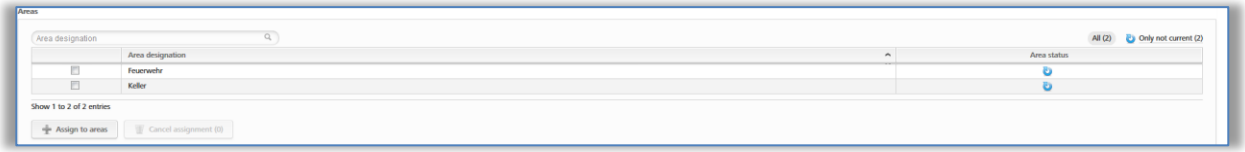
Wskazywany stan baterii odpowiada stanowi w momencie ostatniej aktualizacji lub ostatniego przesłanego wpisu do protokołu. Dlatego może wystąpić sytuacja, w której rzeczywisty stan baterii w komponencie zamykającym będzie odbiegał od stanu baterii wskazanego w Module zarządzania online systemu AirKey.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście kliknąć pozycję komponentu zamykającego, który będzie edytowany.
- W zakładce **Szczegóły** można np. zdefiniować nową nazwę drzwi, opcjonalne informacje dodatkowe ❶ lub wprowadzić lokalizację lub adres komponentu zamykającego. Nastąpi weryfikacja ich jednoznaczności w ramach systemu zamknięć.



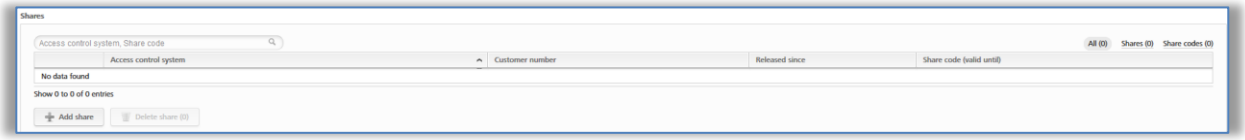
Rys. 132: Edycja komponentu zamykającego

> Przyporządkowania wybranego komponentu zamykającego do stref można edytować w bloku Strefy.



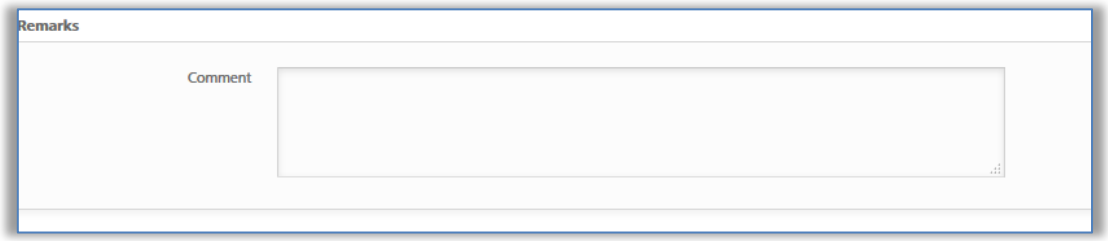
Rys. 133: Strefy

Opcjonalnie można udostępnić komponent zamykający w innych systemach zamknięć. Administrowanie udostępnieniami odbywa się w bloku Zezwolenia. Bliższe informacje na temat zezwoleń i udostępniania znajdują się w rozdziale Praca z kilkoma systemami AirKey.



Rys. 134: Zezwolenia

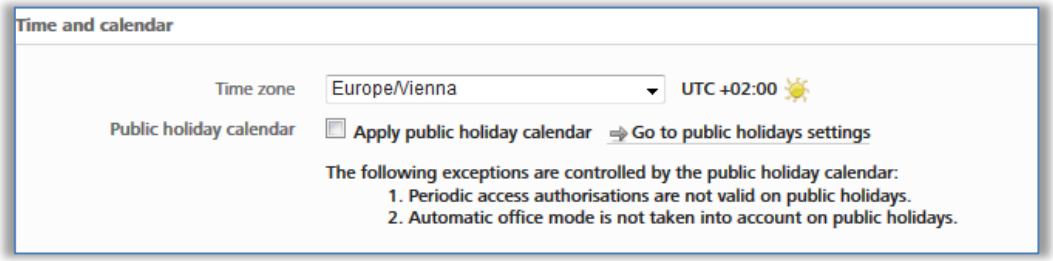
> Opcjonalnie można wprowadzić komentarz na temat komponentu zamykającego w bloku ***Uwagi***.



Rys. 135: Edycja komponentu zamykającego

W zakładce ***Ustawienia*** można – jak wcześniej zostało to wskazane – zarządzać opcjami dotyczącymi strefy czasowej i kalendarza dni świątecznych, a także dostępu, protokołowania i opcji naprawy.

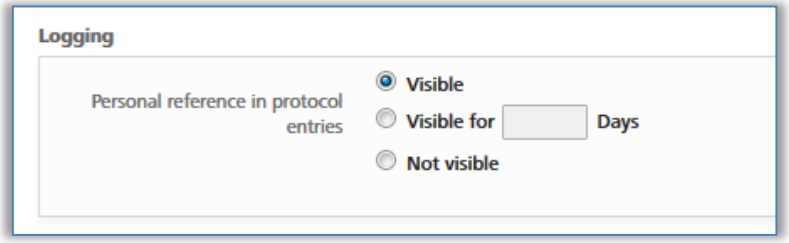
- W przypadku stosowania kilku stref czasowych w ramach jednego systemu zamknięć można przypisać dla każdego komponentu zamykającego własną strefę czasową, która została już utworzona i skonfigurowana w module zarządzania online. Standardowo użyta zostaje strefa czasowa zdefiniowana jako wartość domyślna.
- Kalendarz dni świątecznych można aktywować lub dezaktywować dla każdego komponentu zamykającego. W razie wątpliwości dotyczących konfiguracji dni świątecznych, tutaj znajduje się bezpośredni link do kalendarza dni świątecznych.



Rys. 136: Ustawienia – godzina i kalendarz

- Użytkownik może ustawić ręczne stałe otwarcie dla każdego komponentu zamykającego. Gdy zostanie ono wybrane, pojawi się możliwość aktywacji automatycznego stałego otwarcia.

  Ponadto użytkownik może również zmienić okres zezwolenia lub aktywować / dezaktywować aktualizację po każdej operacji odryglowania. Patrz także rozdział Wartości domyślne (dla wszystkich nowo dodanych komponentów zamykających).
- W przypadku każdego komponentu zamykającego użytkownik ma możliwość dopasowania relacji osobowych we wpisach do protokołu. Standardowo przyjęta zostaje wartość domyślna z ustawień.
  - ***Widoczne*** pozwala na wyświetlanie danych osobowych ze zdarzeń dostępowych bez ograniczenia czasowego.
  - ***Widoczne przez ... dni*** spowoduje anonimizację danych osobowych ze zdarzeń dostępowych po określonej liczbie dni.
  - ***Niewidoczne*** spowoduje anonimizację wszystkich danych osobowych ze zdarzeń dostępowych.



Rys. 137: Protokołowanie

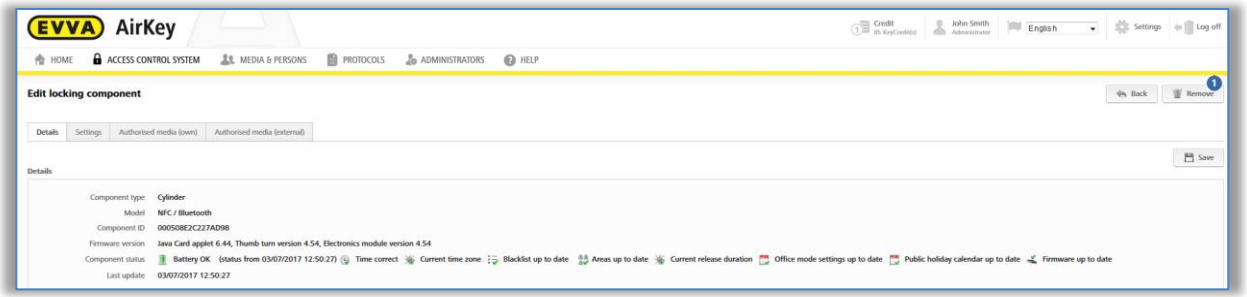
- Tutaj znajduje się także link do opcji naprawy. Bliższe informacje o opcjach naprawy można znaleźć w rozdziale Opcje naprawy.
- Kliknąć przycisk ***Zapisz***, aby przyjąć zmiany w komponencie zamykającym. Następnie pojawi się komunikat o pomyślnym wykonaniu operacji.

W zależności od tego, jakie dane komponentu zamykającego były edytowane, może powstać zadanie konserwacyjne dla danego komponentu zamykającego. Poprzez aktualizację komponentu zamykającego za pomocą smartfona z uprawnieniem do trybu konserwacji lub za pomocą stacji kodującej następuje przejęcie zmian i zadanie konserwacyjne zniknie.

5.5.4 Usuwanie komponentu zamykającego

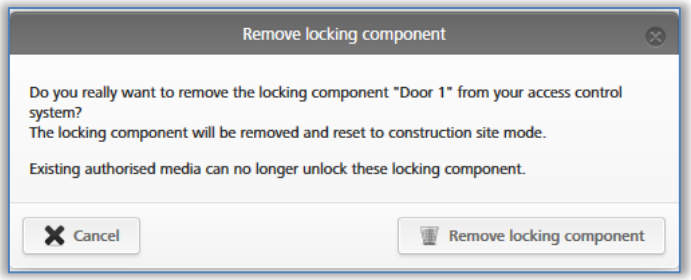
Jeśli dany komponent zamykający nie jest już potrzebny w systemie AirKey, można go usunąć z systemu.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Kliknąć pozycję listy komponentu zamykającego, który będzie usunięty z systemu zamknięć.
- Kliknąć przycisk ***Usuń*** ❶z prawej strony, na górze ekranu.



Rys. 138: Usuwanie komponentu zamykającego

- Potwierdzić pytanie bezpieczeństwa przyciskiem ***Usunąć komponent zamykający***.



Rys. 139: Pytanie bezpieczeństwa

- Pojawi się komunikat o pomyślnym wykonaniu operacji oraz zadanie konserwacyjne dotyczące konieczności usunięcia komponentu zamykającego z systemu zamknięć.

Procedura jest całkowicie ukończona dopiero wówczas, gdy komponent zamykający będzie zaktualizowany za pomocą smartfona z uprawnieniem do trybu konserwacji lub za pomocą opcjonalnej stacji kodującej. Gdy komponent zamykający zostanie zaktualizowany, nastąpi jego pomyślne usunięcie z systemu zamknięć.

Ta operacja nie może być anulowana.

Komponent zamykający po usunięciu zostanie przywrócony do stanu fabrycznego.

Za pomocą wcześniej uprawnionych nośników dostępu nie można już odryglować komponentu zamykającego. Odpowiednie uprawnienia zostaną automatycznie usunięte i już nie będą wyświetlane.

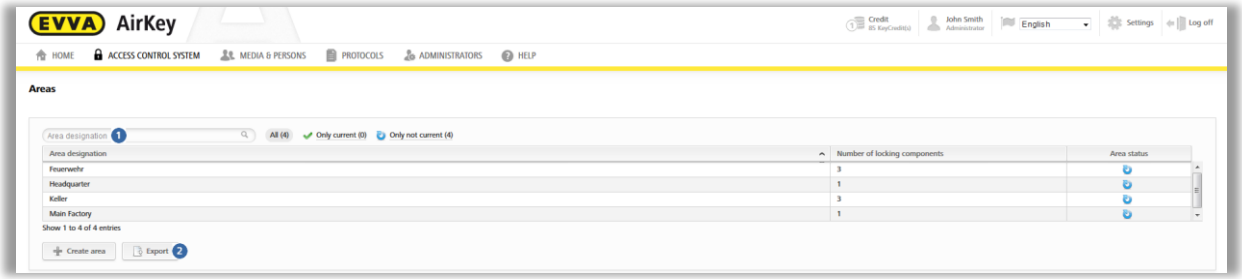
5.5.5 Strefy

Kilka komponentów zamykających można pogrupować w strefy. Dzięki temu zarządzanie uprawnieniami w określonym systemie zamknięć jest znacznie prostsze.

Na stronie startowej ***Home*** w obszarze ***Strefy*** lub w menu głównym ***System zamknięć*** → ***Strefy*** można uzyskać listę wszystkich stref łącznie z ich statusem.

Na wyświetlonej liście stref użytkownik może wykonać następujące operacje:

- Wprowadzić w polu wyszukiwania ❶ kryterium wyszukiwania zawierające co najmniej trzy znaki.
- Kliknąć wybrany nagłówek kolumny, aby zastosować go jako kryterium sortowania.
- Listę stref można eksportować do pliku CSV w celu dalszego przetwarzania ❷.



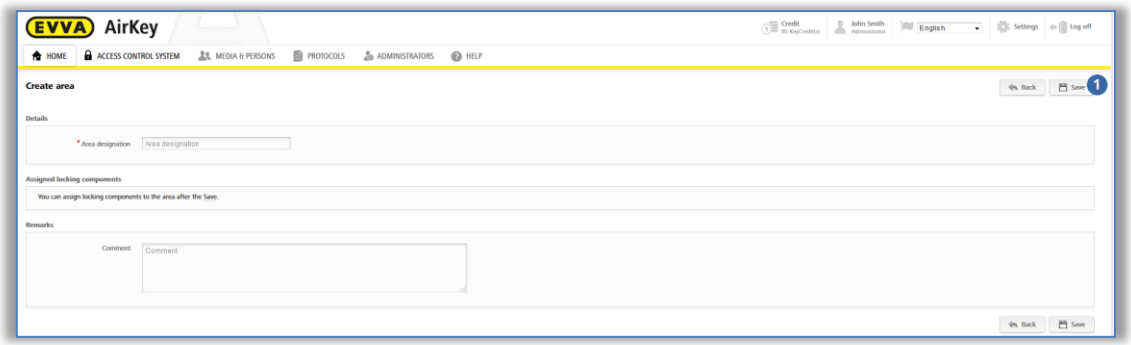
Rys. 140: System zamknięć – Strefy

- Wybrać z listy żądaną strefę, aby wyświetlić informacje szczegółowe na jej temat.

5.5.6 Utworzenie strefy

Standardowo w systemie żadna strefa nie jest wstępnie utworzona. Użytkownik musi utworzyć nowe strefy, aby móc dodawać komponenty zamykające w ramach stref.

- Na stronie startowej ***Home*** na szarym pasku bloku ***System zamknięć*** kliknąć ***Dodaj*** → ***Utwórz strefę***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Utwórz strefę***.
- Wprowadzić charakterystyczną nazwę strefy.
- Bliższe informacje na temat strefy można zamieścić w bloku ***Uwagi*** w polu ***Komentarz***.
- Kliknąć przycisk ***Zapisz*** ❶.

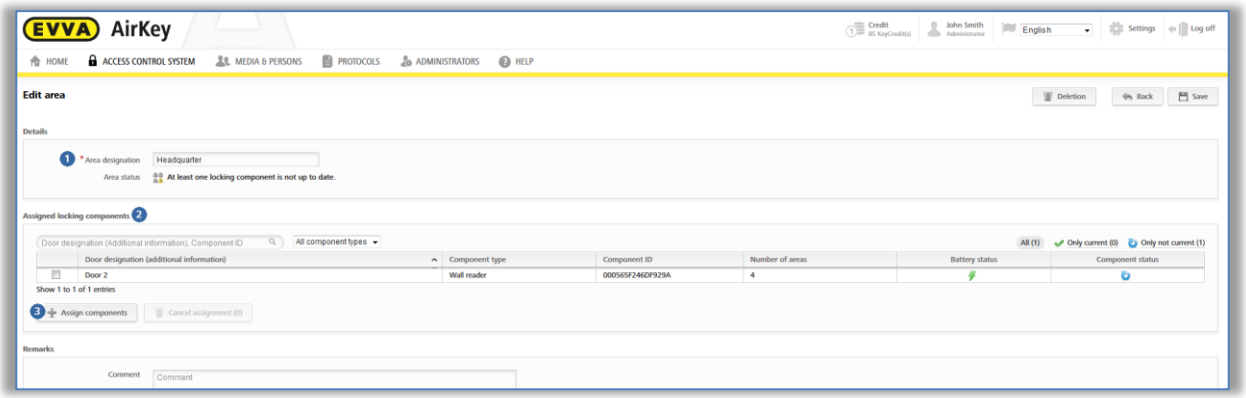


Rys. 141: Utworzenie strefy

Pomyślne utworzenie strefy będzie potwierdzone komunikatem "Strefa została zapisana". Komponenty zamykające można dodać do strefy dopiero wówczas, gdy zostanie ona pomyślnie zapisana.

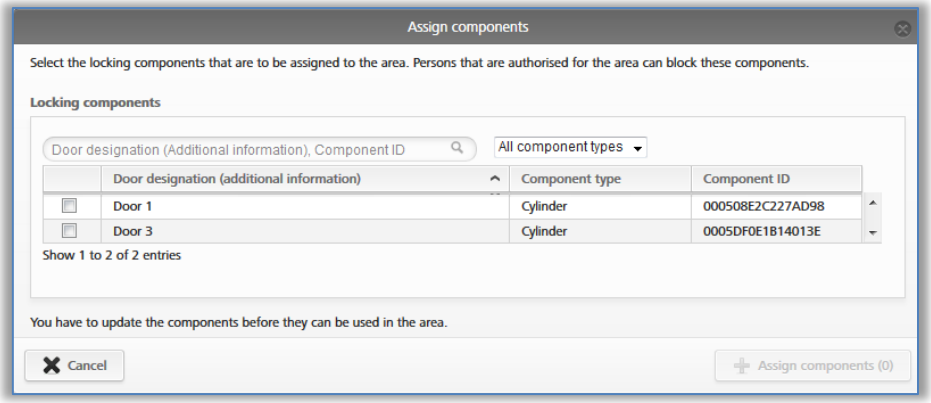
5.5.7 Przypisanie komponentów zamykających do stref

- Na stronie startowej ***Home*** wybrać ikonę ***Strefy*** lub w menu głównym ***System zamknięć*** → ***Strefy***.
- Wybrać z listy strefę, do której zostanie dodany komponent zamykający.
- Pojawią się informacje szczegółowe na temat wybranej strefy. Pole ***Stan strefy*** ❶ wskazuje, czy wszystkie komponenty zamykające w danej strefie są aktualne. Blok ***Przypisane komponenty zamykające*** ❷ zawiera wszystkie komponenty zamykające przypisane do danej strefy.
- Kliknąć opcję ***Przypisz komponenty*** ❸, aby przyjąć komponent zamykający do strefy.



Rys. 142: Edycja strefy

Zostanie wyświetlona lista wszystkich komponentów zamykających, które nie są przypisane do tej strefy.



Rys. 143: Przypisanie komponentów

- Wybrać żądane komponenty zamykające. (Możliwy jest wybór kilku komponentów zamykających, w tym także różnego typu.)
- Kliknąć przycisk ***Przypisz komponenty***, aby przypisać komponenty zamykające do danej strefy.
- Kliknąć przycisk ***Zapisz***, aby zastosować zmiany.

Odnośnie wskazanych komponentów zamykających powstaną zadania konserwacyjne, które można zrealizować poprzez aktualizację określonych komponentów za pomocą smartfona lub stacji kodującej. Po aktualizacjach proces przyporządkowania komponentów zamykających do strefy.

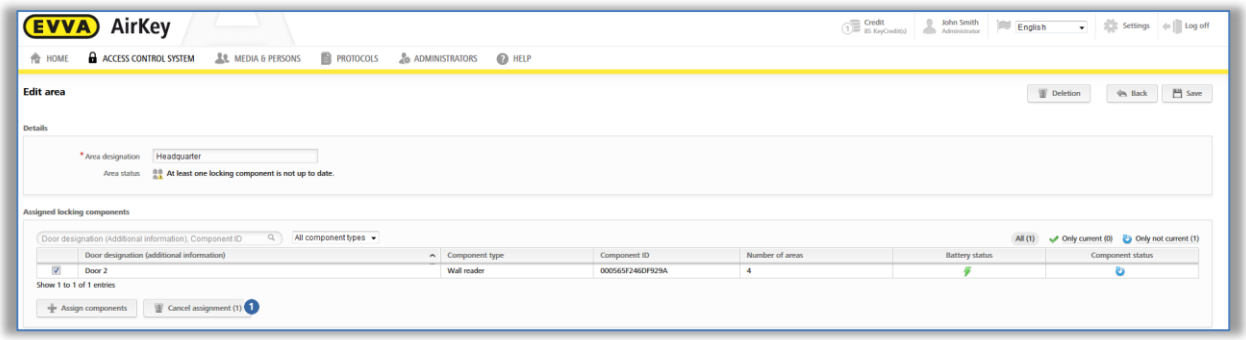
Komponent zamykający można jednocześnie przypisać do maksymalnie 96 stref.

Alternatywnie można także edytować przypisanie strefy dla danego komponentu zamykającego bezpośrednio w sekcji szczegółów komponentu. Bliższe informacje na ten temat można znaleźć w rozdziale Edycja komponentu zamykającego.

5.5.8 Anulowanie przypisania komponentów zamykających do strefy

Aby anulować przypisanie jednego lub kilku komponentów zamykających do strefy, należy wykonać następującą procedurę:

- Na stronie startowej ***Home*** wybrać ikonę ***Strefy*** lub w menu głównym ***System zamknięć → Strefy***.
- Wybrać z listy strefę, dla której nastąpi anulowanie przypisania komponentów zamykających.
- Na liście przypisanych komponentów zamykających zaznaczyć pola wyboru tych komponentów, których przypisanie zostanie anulowane. Możliwy jest wybór kilku komponentów.

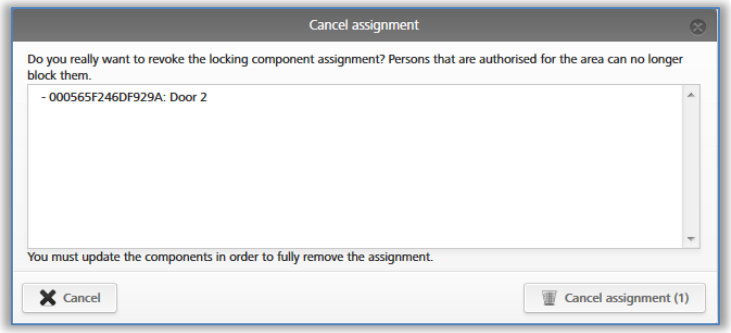


Rys. 144: Zaznaczanie komponentów zamykających

> Kliknąć przycisk ***Anuluj przypisanie*** ❶.

> Pojawi się okno dialogowe z zestawieniem komponentów zamykających, których przypisanie do strefy zostanie anulowane.

> Potwierdzić okno dialogowe przyciskiem ***Anuluj przypisanie***.



Rys. 145: Anulowanie przypisania

Odnośnie wskazanych komponentów zamykających powstaną zadania konserwacyjne, które można zrealizować poprzez aktualizację określonych komponentów za pomocą smartfona lub stacji kodującej. Po aktualizacjach proces przyporządkowania komponentów zamykających do strefy.

Po wykonaniu aktualizacji, osoby, które posiadają nośnik z uprawnieniem do tej strefy, nie mogą już blokować komponentu zamykającego, dla którego anulowano przypisanie.

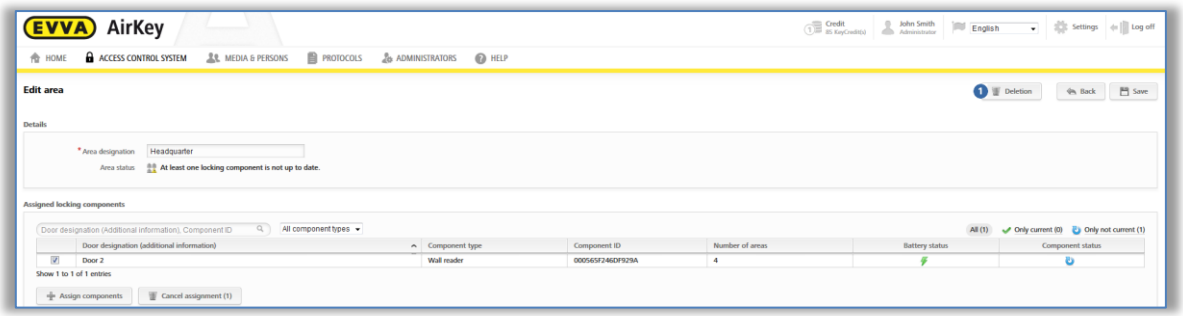
Alternatywnie można także edytować przypisanie strefy dla danego komponentu zamykającego bezpośrednio w sekcji szczegółów komponentu. Bliższe informacje na ten temat można znaleźć w rozdziale Edycja komponentu zamykającego.

5.5.9 Usuwanie strefy

> Na stronie startowej ***Home*** wybrać ikonę ***Strefy*** lub w menu głównym ***System zamknięć*** → ***Strefy***.

> Wybrać z listy strefę, która zostanie usunięta.

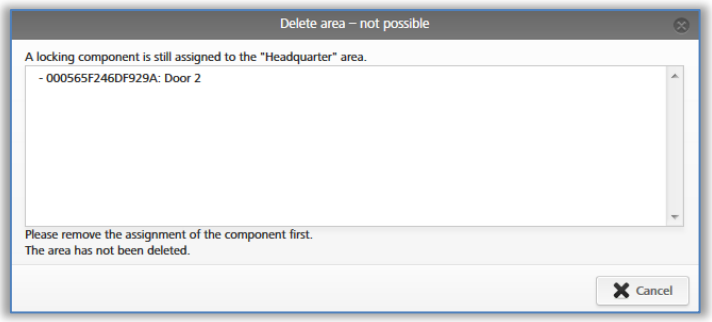
> Kliknąć przycisk ***Usuń*** ❶.



Rys. 146: Usuwanie strefy

W przypadku usuniętej strefy następuje automatyczne skasowanie istniejących uprawnień dla nośnika. Te uprawnienia nie będą już wyświetlane. Kasowanie nie może być anulowane.

Jeśli do danej strefy są jeszcze przypisane komponenty zamykające, zostanie wyświetlony komunikat błędu.



Rys. 147: Usuwanie strefy – niemożliwe

Najpierw należy anulować przypisanie wszystkich komponentów zamykających do danej strefy, a następnie powtórzyć powyższą procedurę. Bliższe informacje na temat anulowania przypisania komponentów zamykających do stref można znaleźć w rozdziale Anulowanie przypisania komponentów zamykających do strefy.

5.5.10 Przegląd uprawnień

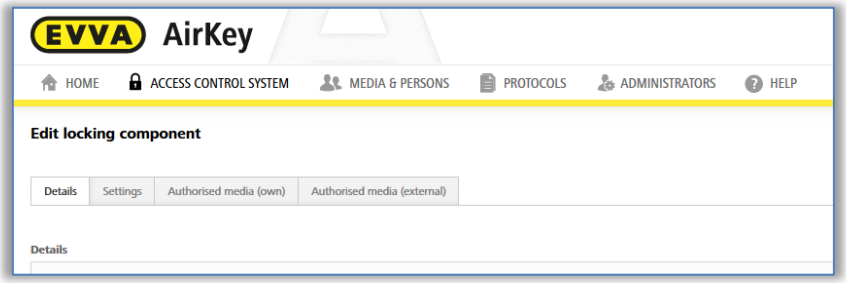
W sekcji przeglądu uprawnień znajduje się lista wszystkich uprawnień nośników względem poszczególnych komponentów zamykających. Przegląd uprawnień odnosi się do wybranego komponentu zamykającego.

Zostanie wyświetlona lista wszystkich nośników, które mają uprawnienia do komponentu zamykającego. Jednak wyświetlone uprawnienia nie muszą być ważne, tzn. nośnik z tymczasowym dostępem pojedynczym w godzinach od 08:00 do 17:00 do określonych komponentów zamykających będzie ujęty w przeglądzie uprawnień także po godzinie 17:00.

> Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny*** lub w menu głównym ***System zamknięć*** → ***Elementy zamykające***.

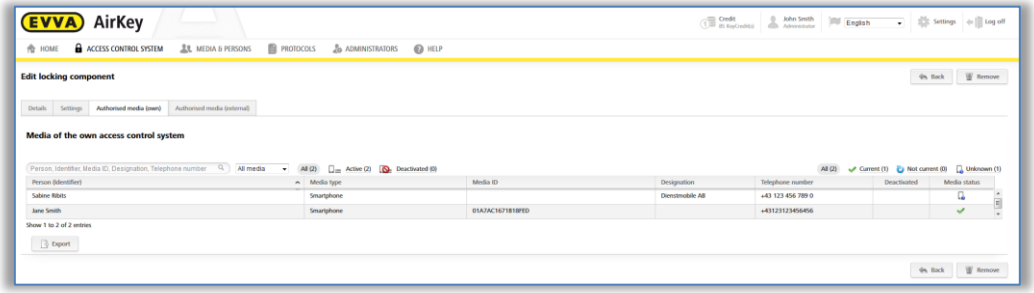
> Wybrać z listy komponent zamykający, dla którego zostanie wyświetlony przegląd uprawnień.

> Przejść z zakładki ***Szczegóły*** do ***Uprawnione nośniki (własne)***, aby przejrzeć uprawnienia własnego systemu zamknięć, lub do ***Uprawnione nośniki (nieznane)***, aby wyświetlić uprawnienia innych systemów, którym komponent zamykający został udostępniony.



Rys. 148: Zakładki strony "Edycja komponentu zamykającego"

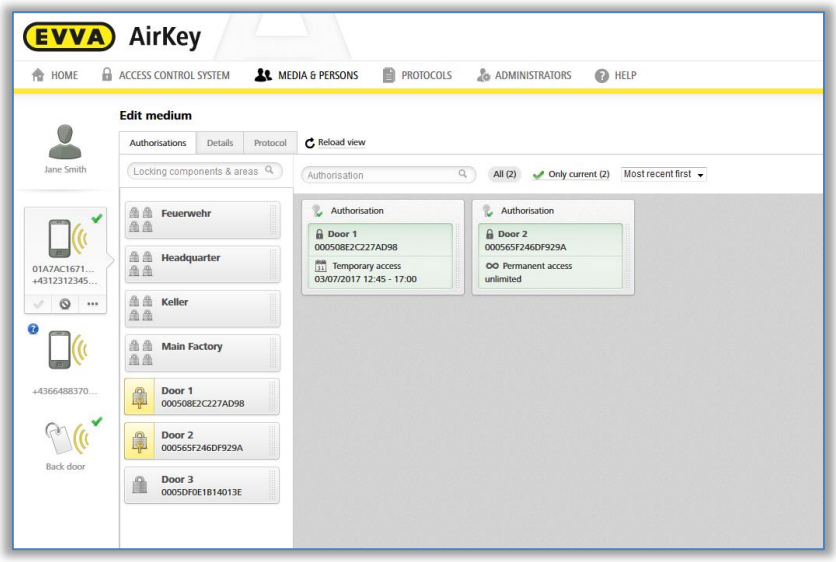
Zostanie wyświetlona lista wszystkich osób wraz z przynależnymi nośnikami. Ponadto wyświetlona będzie informacja o typie nośnika.



Rys. 149: Uprawnione nośniki (własne)

W ramach listy można wykonywać czynności wyszukiwania, filtrowania i sortowania, aby wyszukać określone uprawnienia

Kliknąć nazwisko osoby, aby z przeglądu uprawnień przejść bezpośrednio do uprawnień nośnika danej osoby.



Rys. 150: Edycja nośnika

5.5.11 Zadania konserwacyjne

Pewne funkcje mają wpływ na konfigurację komponentów zamykających. Te zmiany konfiguracji są oznaczone jako zadania konserwacyjne. Zatem zadania konserwacyjne dotyczą komponentów zamykających, których status nie jest aktualny.

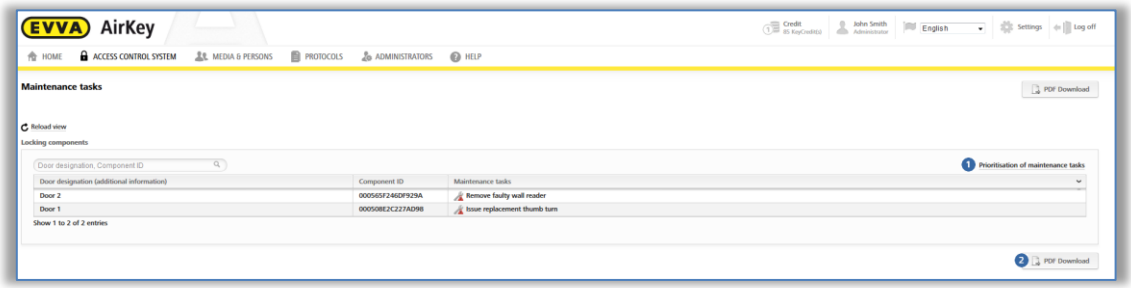
Listę bieżących zadań konserwacyjnych systemu zamknięć AirKey można uzyskać w następujący sposób:

- Na stronie startowej ***Home*** wybrać link ***Zadania konserwacyjne***.
- Alternatywnie można kliknąć na pasku stanu opcję ***Zadania konserwacyjne***.
- Lub w menu głównym wybrać opcje ***System zamknięć → Zadania konserwacyjne***.

Zostanie wyświetlona lista zadań konserwacyjnych dla komponentów zamykających systemu zamknięć AirKey.

Na liście zadań konserwacyjnych możliwe jest wyszukiwanie według oznaczenia drzwi lub identyfikatora komponentu. Można także sortować kolumny "Oznaczenie drzwi (Informacja dodatkowa)", "ID komponentu" i "Zadanie konserwacyjne".

Dodatkowo użytkownik może ustalić priorytety zadań konserwacyjnych ❶ oraz pobrać plik PDF ❷ z wyświetloną listą.



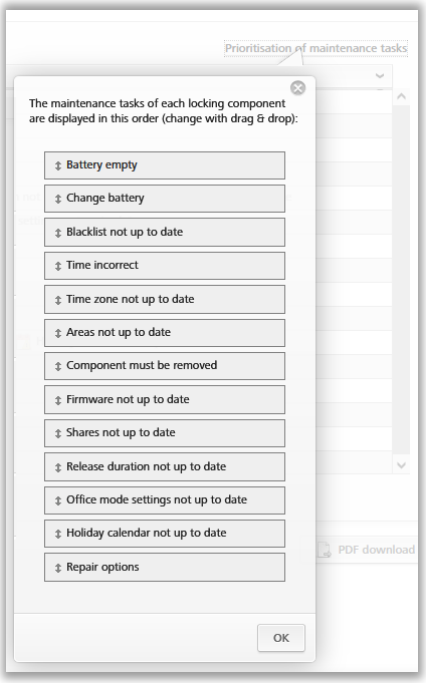
Rys. 151: Zadania konserwacyjne

Ustalanie priorytetów zadań konserwacyjnych jest zapisywane dla każdego systemu zamknięć / klienta i stosuje się je także na smartfonie z zainstalowaną aplikacją AirKey i aktywnym uprawnieniem konserwacyjnym.

> Kliknąć opcję ***Ustalanie priorytetów zadań konserwacyjnych***.

> W zależności od zastosowania i potrzeb klientów można przeciągnąć pozycje metodą "przeciągnij i upuść" ❶ i ułożyć w żądanej kolejności.

> Zapisać zmodyfikowaną listę priorytetów za pomocą przycisku ***OK***.



Rys. 152: Ustalanie priorytetów zadań konserwacyjnych

Zostanie wyświetlona lista zadań konserwacyjnych uwzględniająca zmianę priorytetów. Poszczególne pozycje na liście zadań konserwacyjnych są powiązane z sekcją szczegółów określonego komponentu zamykającego.

Po wykonaniu zadania konserwacyjnego (aktualizacji komponentu zamykającego) określona pozycja automatycznie znika z listy zadań konserwacyjnych.

Listę wszystkich oczekujących zadań konserwacyjnych można zapisać jako plik PDF i wydrukować. W tym celu należy skorzystać z przycisku ***PDF do pobrania***.

5.5.12 Dane klienta – plan dostępów

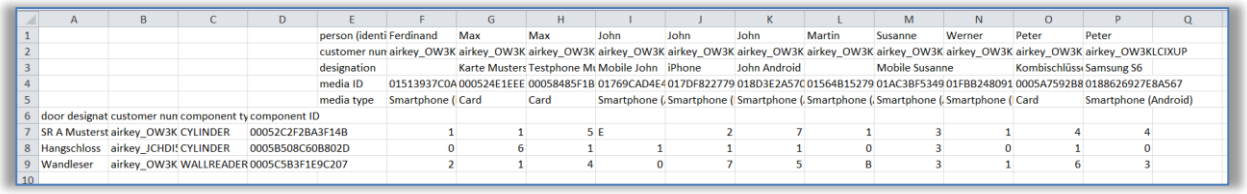
Jak już wcześniej wspomniano, w menu ***Dane klienta*** można zmienić różne informacje, które zostały wprowadzone podczas rejestracji. Dotyczy to np. nazwy systemu zamknięć, nazwy firmy lub osoby do kontaktu.

Na ekranie "Edytuj dane klienta" z prawej strony znajduje się przycisk, za pomocą którego można wyeksportować plan dostępów dla całego systemu zamknięć. Plan dostępów to zestawienie wszystkich komponentów zamykających w systemie zamknięć wraz z przypisanymi do nich smartfonami i nośnikami dostępu.

> Kliknąć przycisk ***Eksportuj plan dostępów***.

> W oknie dialogowym "Eksportuj plan dostępów" wybrać przycisk ***Eksportuj***.

- Kliknąć link pliku CSV, który pojawi się w kolejnym oknie dialogowym.
- Otworzyć plik CSV za pomocą wybranego programu lub zapisać plik.
- Zamknąć okno dialogowe "Eksportuj plan dostępów", klikając przycisk ***Zamknij***.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1					person (identi	Ferdinand	Max	Max	John	John	John	Martin	Susanne	Werner	Peter	Peter	
2					customer nun	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3KLCIXUP	
3					designation		Karte Musters	Testphone M	Mobile John	iPhone	John Android		Mobile Susanne		Kombischlüss	Samsung S6	
4					media ID	01513937C0A	000524E1EEE	00058485F1B	01769CAD4E4	017DF822779	018D3E2A57C	01564B15279	01AC3BF5349	01FBB248091	0005A7592B8	0188626927E8A567	
5					media type	Smartphone (	Card	Card	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Card	Smartphone (Android)	
6	door designat	customer nun	component ty	component ID													
7	SR A Musterst	airkey_OW3K	CYLINDER	00052C2F2BA3F14B		1	1	5	E	2	7	1	3	1	4	4	
8	Hangschloss	airkey_JCHDI	CYLINDER	0005B508C60B802D		0	6	1	1	1	1	0	3	0	1	0	
9	Wandleser	airkey_OW3K	WALLREADER	0005C5B3F1E9C207		2	1	4	0	7	5	B	3	1	6	3	
10																	

Rys. 153: Plan dostępów

Zostanie odczytany stan Modułu zarządzania online systemu AirKey do przeliczenia stanu uprawnień, a nie RZECZYWISTY stan dla nośnika. To oznacza, że plan dostępów będzie prawidłowy tylko wówczas, gdy wszystkie komponenty i nośniki są aktualne.

Legenda planu dostępów:

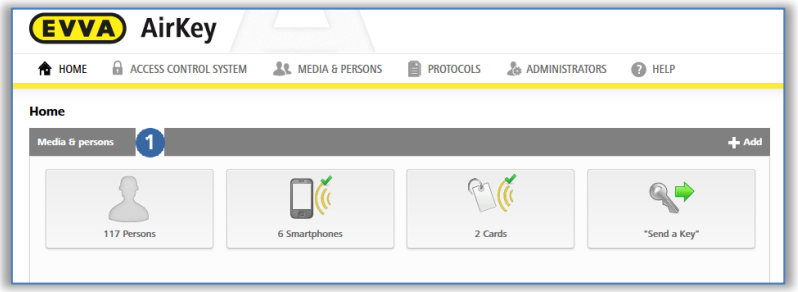
- **0** – **Brak uprawnienia**: Nośnik nie ma uprawnienia dla komponentu zamykającego i dla żadnej strefy, do której należy komponent zamykający.
- **1** – **Uprawnienie stałe bez daty upływu ważności**: Nośnik ma dokładnie jedno stałe uprawnienie bez daty upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.
- **2** – **Uprawnienie stałe z datą upływu ważności**: (1) nie ma zastosowania i nośnik ma dokładnie jedno stałe uprawnienie z przyszłą datą upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.
- **3** – **Okresowe uprawnienie bez daty upływu ważności**: (1) i (2) nie mają zastosowania i nośnik ma dokładnie jedno okresowe uprawnienie bez daty upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.
- **4** – **Okresowe uprawnienie z datą upływu ważności**: (1), (2) i (3) nie mają zastosowania i nośnik ma dokładnie jedno okresowe uprawnienie z przyszłą datą upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.
- **5** – **Uprawnienie jednorazowe**: (1), (2), (3) i (4) nie mają zastosowania i nośnik ma dokładnie jedno uprawnienie jednorazowe z przyszłą datą upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.
- **6** – **Uprawnienie indywidualne**: (1), (2), (3), (4) i (5) nie mają zastosowania i nośnik ma dokładnie jedno uprawnienie indywidualne z co najmniej jednym upraw-

nieniem podrzędnym i z przyszłą datą upływu ważności dla komponentu zamykającego lub strefy, do której należy komponent zamykający, i nie ma żadnych dalszych uprawnień dla komponentu zamykającego lub strefy, do której należy komponent zamykający.

- **7 – Uprawnienie wielokrotne**: Nośnik ma co najmniej dwa uprawnienia dla komponentu zamykającego lub strefy, do której należy komponent zamykający, których ważność jeszcze nie upłynęła.
- **B – Czarna lista**: Nośnik jest dezaktywowany, tzn. został wpisany na czarną listę komponentów zamykających. Z tego powodu uprawnienia tego nośnika tracą ważność.
- **E – Uprawnienie nieważne (każdego typu)**: Wszystkie uprawnienia nośnika dla komponentu zamykającego lub strefy, do której należy komponent zamykający, utraciły ważność.

5.6 Nośniki i osoby

Menu główne ***Nośniki i osoby*** ❶ służy do zarządzania wszystkimi osobami, nośnikami i ich uprawnieniami w systemie zamknięć AirKey.



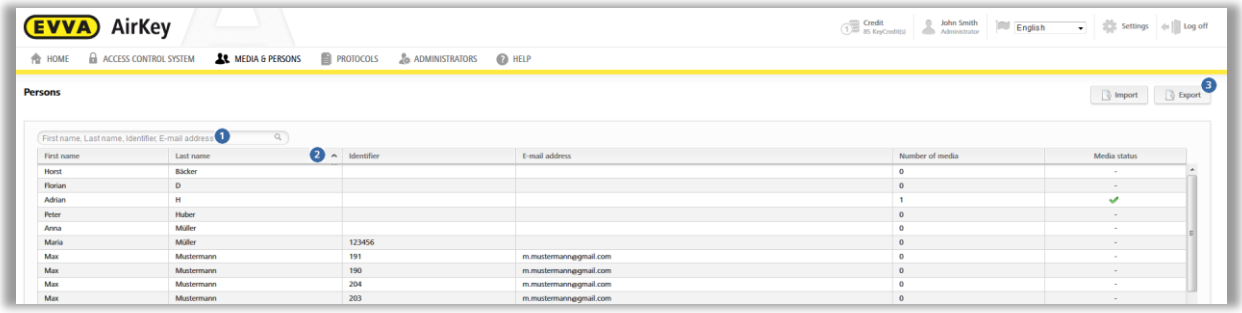
Rys. 154: Nośniki i osoby

5.6.1 Przegląd osób

Po wybraniu na stronie startowej ***Home*** ikony ***Osoby*** lub w menu głównym opcji ***Nośniki i osoby*** → ***Osoby***, zostanie wyświetlona lista wszystkich utworzonych osób łącznie z liczbą nośników oraz statusem nośników.

Na wyświetlonej liście użytkownik może wykonać następujące operacje:

- Wprowadzić w polu wyszukiwania ❶ kryterium wyszukiwania zawierające co najmniej 3 znaki.
  Do wyboru jest imię, nazwisko, identyfikator lub adres e-mail.
- Kliknąć wybrany nagłówek kolumny, aby zastosować go jako kryterium sortowania ❷.
- Można także wyeksportować całą listę do pliku CSV w celu dalszego przetwarzania ❸.



Rys. 155: Osoby

5.6.2 Utworzenie osoby: patrz rozdział 4.7

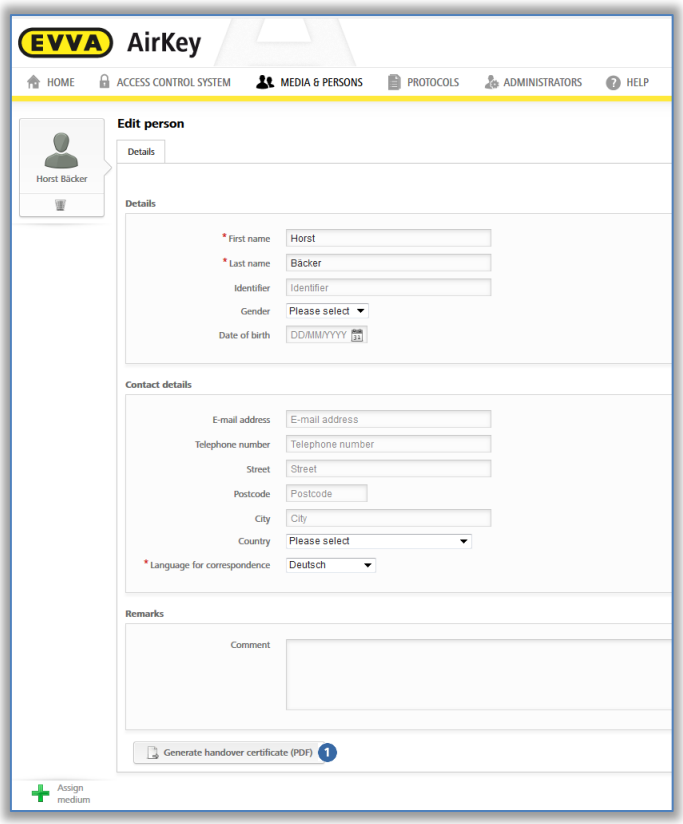
5.6.3 Edycja osoby

W widoku szczegółowym "Edycja osoby" użytkownik może zmienić szczegóły i dane kontaktowe określonej osoby, a także może przypisać jej nowy nośnik.

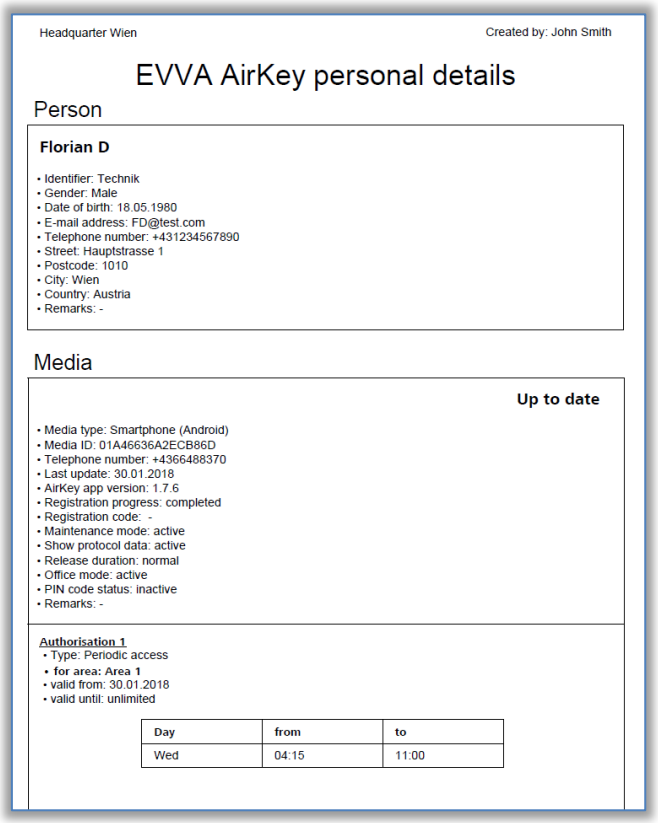
- Na stronie startowej ***Home*** wybrać ikonę ***Osoby***.
- Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Osoby***.
- Na liście osób kliknąć nazwisko osoby, której dane zostaną zmienione.
- Zmienić odpowiednie dane.
- Kliknąć przycisk ***Zapisz***.

Na ekranie "Edycja osoby" można także utworzyć potwierdzenie przekazania ❶. Jest to potwierdzenie, które po utworzeniu i przypisaniu wszystkich niezbędnych uprawnień zostaje przekazane osobie. Potwierdzenie wskazuje, które nośniki z jakimi uprawnieniami w momencie utworzenia są w posiadaniu danej osoby.

- Z listy przeglądu wybrać osobę, dla której ma zostać wystawione potwierdzenie przekazania.
- Na ekranie "Edycja osoby" kliknąć przycisk ***Generowanie certyfikatu odbioru (PDF)***.
- Pojawi się okno dialogowe "Generowanie certyfikatu odbioru (PDF)", w którym plik PDF będzie udostępniony za pośrednictwem linku.
- Kliknąć link i otworzyć plik PDF za pomocą programu PDF Reader lub zapisać plik.
- Zamknąć okno dialogowe, naciskając przycisk ***Zamknij***.



Rys. 156: Generowanie certyfikatu odbioru



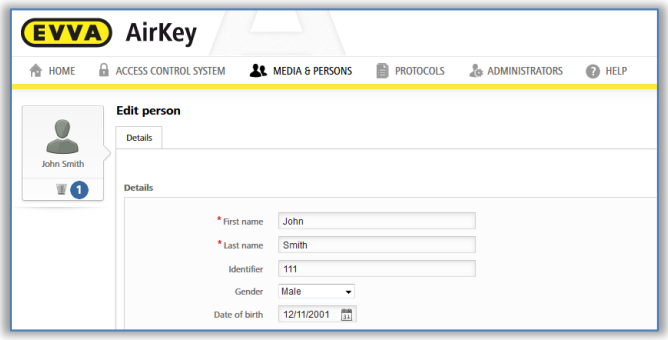
Rys. 157: Certyfikatu odbioru (PDF)

5.6.4 Kasowanie osoby

Istnieje możliwość usunięcia osoby z systemu AirKey.

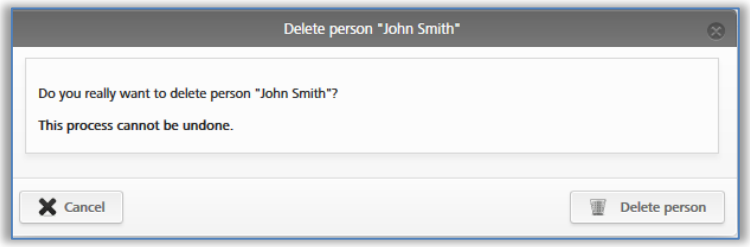
Osoba, która ma jeszcze przypisane nośniki, nie może zostać usunięta. Dlatego należy pamiętać, aby przed usunięciem anulować przypisanie wszystkich nośników do wybranej osoby.

> Na stronie startowej ***Home*** wybrać ikonę ***Osoby***.
> Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Osoby***.
> Na liście osób kliknąć nazwisko osoby, która zostanie usunięta.
> Kliknąć symbol ***kosza*** ❶.



Rys. 158: Kasowanie osoby

> Potwierdzić pytanie bezpieczeństwa przyciskiem Usuń osobę.



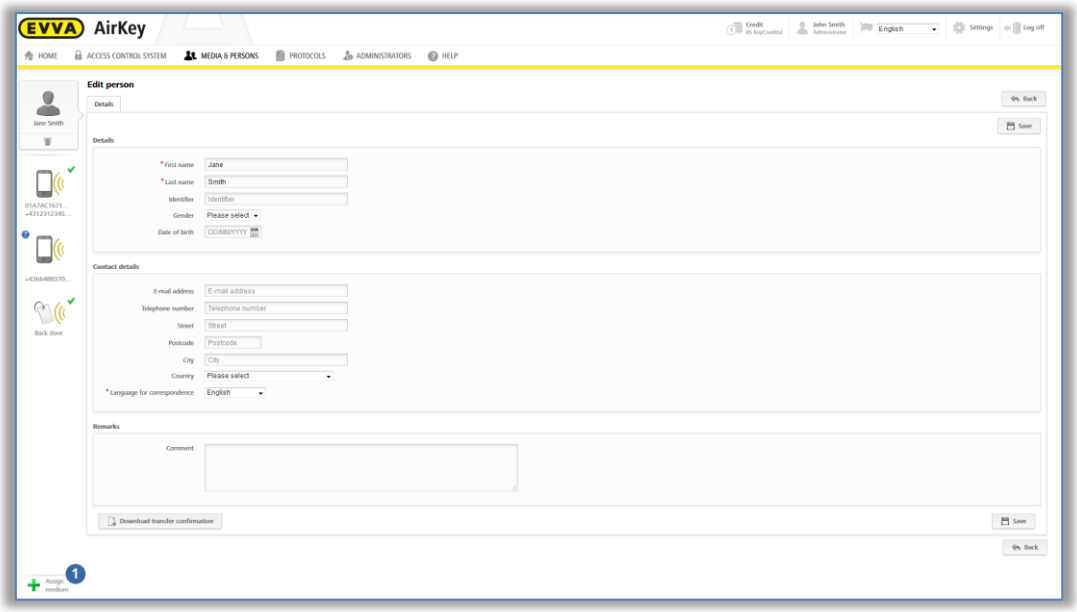
Rys. 159: Kasowanie osoby – pytanie bezpieczeństwa

Skasowana osoba nie będzie ujęta na liście osób. Wpisy do protokołu sprzed skasowania osoby będą nadal dokumentować relację osobową względem komponentów zamykających i nośników.

5.6.5 Przypisanie nośnika do osoby

Aby możliwe było przypisywanie uprawnień, należy przypisać nośnik do osoby. Tylko w ten sposób można uzyskać relację osobową w przypadku dostępów.

> Na stronie startowej ***Home*** wybrać ikonę ***Osoby***.
> Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Osoby***.
> Na liście osób kliknąć nazwisko osoby, do której zostanie przypisany nośnik.
> Kliknąć przycisk ***Przypisz nośnik*** ❶.

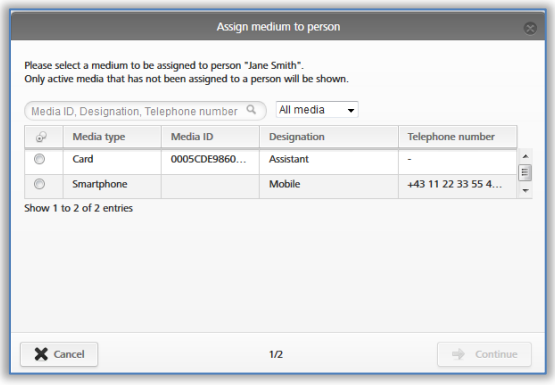


Rys. 160: Przyporządkowanie nośnika

Zostanie wyświetlona lista z wszystkimi nośnikami, które można przypisać danej osobie. W ramach listy możliwe jest sortowanie, filtrowanie według typu nośnika lub wyszukiwanie według określonych pozycji.

Wyświetlane będą wyłącznie nośniki danego systemu, które jeszcze nie zostały przypisane żadnej osobie.

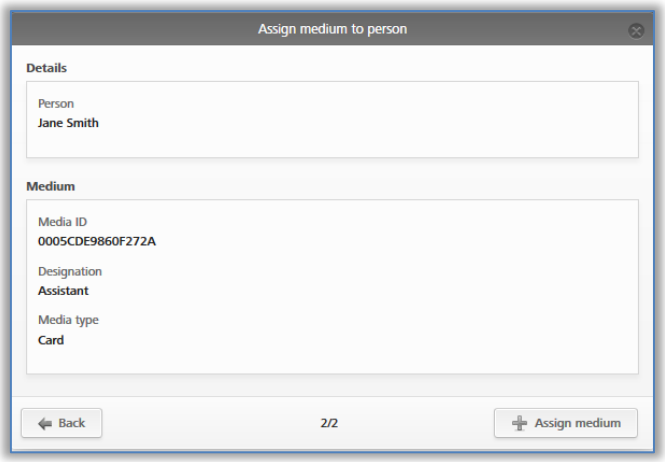
> Wybrać żądany nośnik i kliknąć przycisk ***Dalej***.



Rys. 161: Przypisanie nośnika do osoby

Po wybraniu nośnika zostaną wyświetlone informacje szczegółowe. W razie potrzeby należy kliknąć przycisk Wstecz i wybrać inny nośnik.

> Kliknąć przycisk ***Przypisz nośnik***, aby zakończyć operację.



Rys. 162: Przypisanie nośnika do osoby

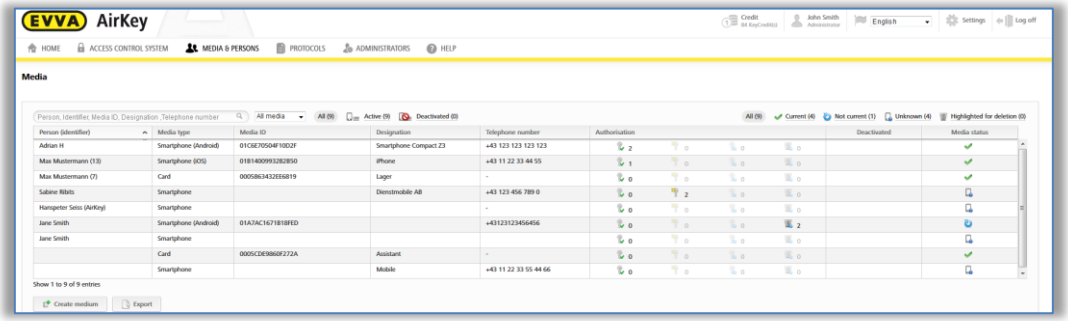
Alternatywnie można wykonać przypisanie nośnika danej osobie za pomocą danych nośnika. Bliższe informacje na ten temat znajdują się w rozdziale Przypisanie osoby do nośnika.

Możliwe jest przypisanie kilku nośników (smartfony, karty, breloki do kluczy lub klucze Combi) do jednej osoby.

5.6.6 Przegląd nośników

W menu głównym ***Nośniki i osoby*** → ***Nośniki*** znajduje się lista wszystkich nośników (smartfony, karty, breloki do kluczy i klucze Combi), umożliwiająca przegląd przyznanych uprawnień, ewentualnych dezaktywacji oraz aktualnego statusu nośników.

W ramach listy nośników użytkownik może wyszukiwać określone nośniki, filtrować według wybranego statusu, zmieniać sortowanie lub wyeksportować całą listę do pliku CSV.



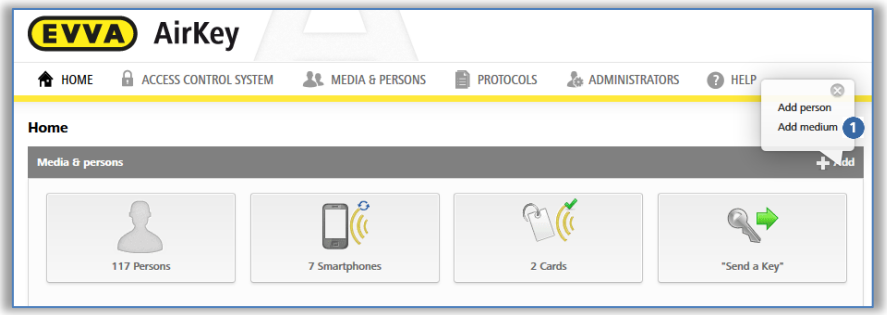
Rys. 163: Lista nośników

5.6.7 Utworzenie nośnika

Aby zarządzać nośnikami w ramach systemu zamknięć, najpierw należy je utworzyć w systemie.

- Na stronie startowej ***Home*** na szarym pasku bloku ***Nośniki i osoby*** kliknąć ***Dodaj*** → ***Dodaj nośnik***.
- Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Dodaj nośnik***.

> Lub na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***, a następnie ***Dodaj nośnik***.



Rys. 164: Utworzenie nośnika

> Wybrać typ nowego nośnika.

Rys. 165: Utworzenie nowego nośnika

Karty, breloki do kluczy, bransoletki oraz klucze Combi z perspektywy aplikacji nie są rozróżniane, dlatego w przypadku breloka lub klucza Combi należy wskazać typ nośnika jako ***Karta***.

5.6.8 Utworzenie smartfona: patrz rozdział 4.8

5.6.9 Utworzenie karty, breloka do kluczy, bransoletki lub klucza Combi

Jeśli użytkownik nie dysponuje stacją kodującą, do systemu można dodawać karty, breloki do kluczy, bransoletki lub klucze Combi za pomocą smartfona z uprawnieniem do konserwacji. W tym celu należy postępować zgodnie z instrukcjami zawartymi w rozdziale Dodawanie kart, breloków do kluczy i kluczy Combi za pomocą smartfona.

> Wprowadzić oznaczenie i kliknąć przycisk ***Dalej***.

> Położyć kartę, brelok do kluczy lub klucz Combi na stacji kodującej.

Jeśli operacja zostanie pomyślnie zakończona, automatycznie otworzy się widok szczegółów tego nośnika.

Wyraźnie zaleca się przygotowanie wystarczającej liczby wstępnie skonfigurowanych nośników (karty, breloki do kluczy, bransoletki lub klucze Combi) ze uprawnieniami dostępu bez daty upływu ważności (nośniki awaryjne) oraz ich przechowywanie w bezpiecznych miejscach, aby możliwa

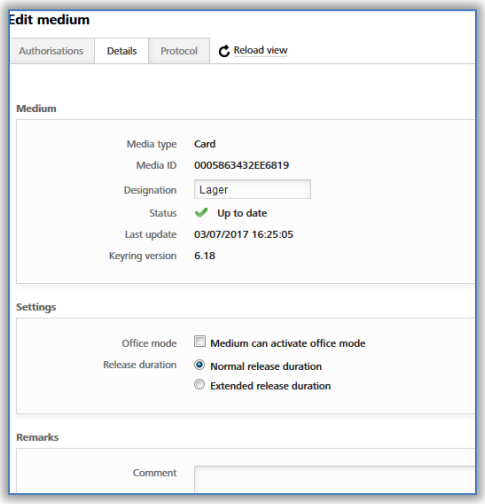
była eksploatacja systemu zamknięć także niezależnie od modułu zarządzania online. Informacje na temat przekazywania uprawnień można znaleźć w rozdziale Uprawnienia.

Dodanie klucza Combi za pomocą stacji kodującej należy wykonać na tej stronie klucza, na której znajduje się symbol RFID. Klucz Combi należy trzymać bezpośrednio przy stacji kodującej. Operacja dodawania nie jest możliwa na całym obszarze czytnika stacji kodującej – w przypadku aktualnej wersji (HID Omnikey 5421) klucz Combi będzie wykryty tylko w górnej i dolnej jednej trzeciej części stacji kodującej.

Sposób dodawania nośników za pomocą smartfona z uprawnieniem konserwacyjnym do systemu AirKey opisano w rozdziale Dodawanie kart, breloków do kluczy i kluczy Combi za pomocą smartfona.

5.6.10 Edycja nośnika

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć żądany nośnik.
- Wybrać zakładkę ***Szczegóły*** w celu edycji danych nośnika.



Rys. 166: Edycja nośnika – karta

- Kliknięcie przycisku ***Zapisz*** spowoduje zastosowanie zmian.

5.6.11 Przypisanie osoby do nośnika: patrz rozdział 4.13

5.6.12 Uprawnienia

Uprawnienia regulują dostęp osób do komponentów zamykających. Aby utworzyć uprawnienia dla nośników, nośniki muszą zostać wcześniej przypisane osobie (bliższe informacje na temat przypisywania nośnika do osoby znajdują się w rozdziale Przypisanie nośnika do osoby).

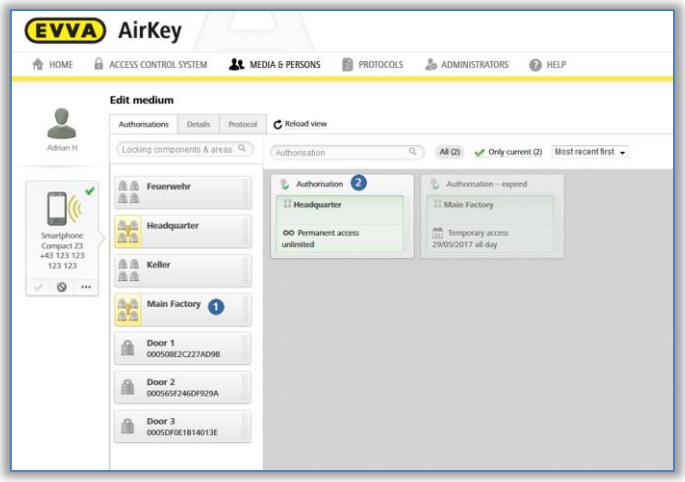
Przegląd uprawnień nośnika można uzyskać w następujący sposób:

> Wybrać w menu głównym opcje ***Nośniki i osoby*** → ***Nośniki***.

> Na liście przeglądu kliknąć żądany nośnik.

> Nośnik ❶ został już wybrany (jednej osobie można przypisać kilka nośników).

> Zostaną wyświetlone wszystkie już udzielone uprawnienia ❷.



Rys. 167: Przegląd uprawnień

Kolor tła uprawnień:

- ***Zielony*** = status jest aktualny, uprawnienie zostało potwierdzone i nośnik zaktualizowany.
- ***Niebieski*** = uprawnienie zostało potwierdzone, nośnik jeszcze nie został zaktualizowany.
- ***Żółty*** = uprawnienie zostało zmienione lub usunięte, ale jeszcze nie zostało potwierdzone.
- ***Szary*** = ważność uprawnienia upłynęła.

Alternatywnie można wywołać przegląd uprawnień poprzez menu główne ***Nośniki i osoby*** → ***Osoby***, wybierając z listy osób osobę, która posiada nośnik. Następnie należy kliknąć symbol nośnika z lewej strony, poniżej wybranej osoby.

5.6.13 Przydzielanie uprawnień: patrz rozdział 4.14

5.6.14 Potwierdzenie uprawnienia: patrz rozdział 4.15

5.6.15 Zmiana uprawnienia

Uprawnienia można zmieniać poprzez Moduł zarządzania online systemu AirKey w dowolnym momencie.

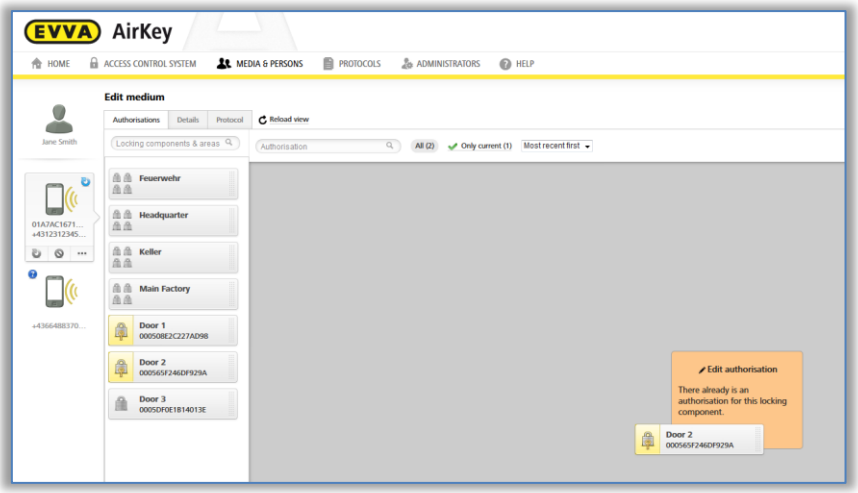
> Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.

> Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.

> Na liście przeglądu kliknąć nośnik, dla którego nastąpi zmiana uprawnień.

> W zakładce "Uprawnienie" kliknąć uprawnienie, które ma zostać zmienione.

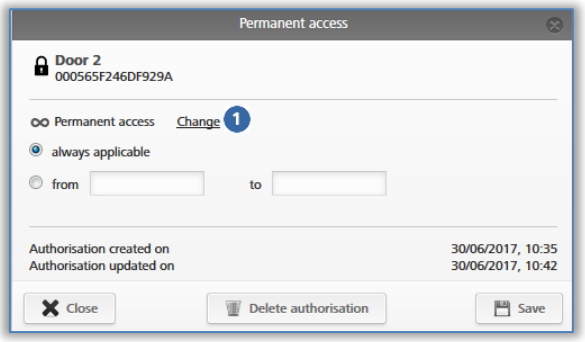
> Alternatywnie można ponownie przeciągnąć i upuścić drzwi / strefę na środkowe pole.



Rys. 168: Edycja nośnika – zmiana uprawnienia

> Zostaną wyświetlone szczegóły istniejącego uprawnienia.

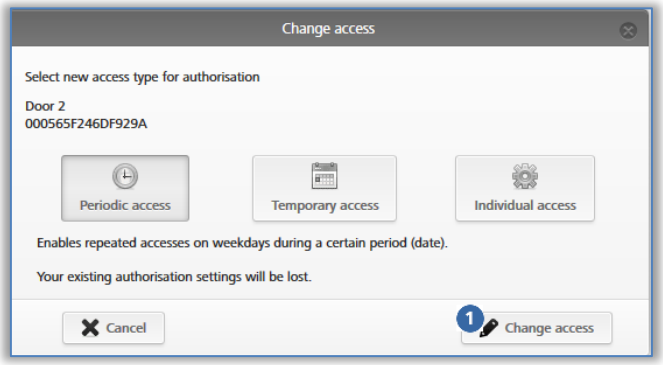
> Kliknąć opcję ***Zmień*** ❶.



Rys. 169: Zmiana uprawnienia

> Wybrać nowy rodzaj dostępu.

> Kliknąć przycisk ***Zmień dostęp*** ❶.



Rys. 170: Zmiana dostępu

> Wprowadzić zmienione wartości do wybranego rodzaju dostępu.

> Kliknąć przycisk ***Zapisz***.

Do zmiany uprawnień wymagane są środki w formie jednostek KeyCredit.

> Kliknąć żółty przycisk ***Utwórz 1 uprawnienie***. Bliższe informacje na ten temat można znaleźć w rozdziale Potwierdzenie uprawnienia.

> Zaktualizować nośnik funkcją "Pull to Refresh" w przypadku smartfona lub za pomocą stacji kodującej w przypadku karty, breloka do kluczy, bransoletką lub klucza Combi, aby pomyślnie zakończyć proces.

5.6.16 Kasowanie uprawnienia

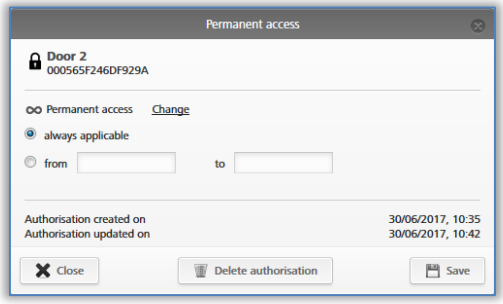
Jeśli istniejące, przyznane uprawnienie nie jest już potrzebne, można je w dowolnym momencie skasować.

> Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.

> Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.

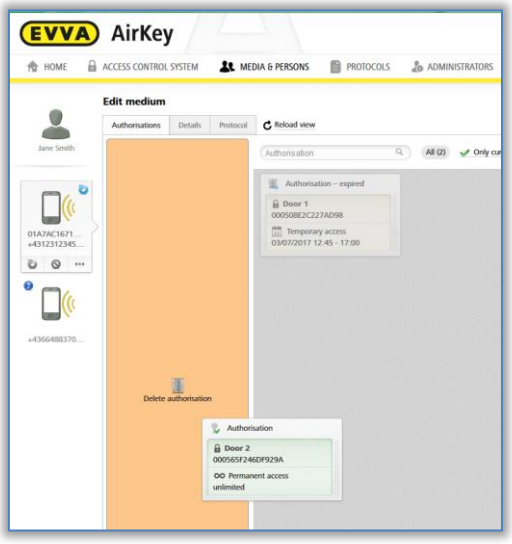
> Na liście przeglądu kliknąć nośnik, dla którego nastąpi skasowanie uprawnień.

> W zakładce "Uprawnienie" kliknąć uprawnienie, które ma zostać skasowane.



Rys. 171: Stały dostęp

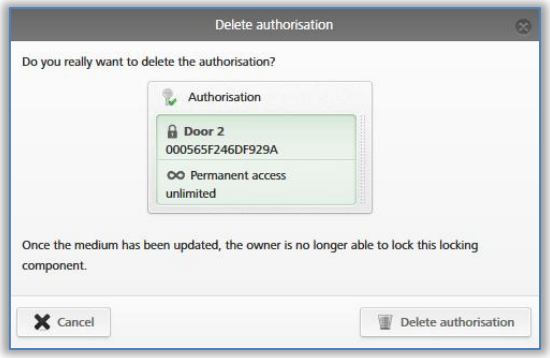
Alternatywnie przeciągnąć i upuścić drzwi / strefę ze środkowego pola na pomarańczowe pole ***Skasuj uprawnienie***.



Rys. 172: Skasowanie uprawnienia

> Kliknąć przycisk ***Skasuj uprawnienie***.

> Potwierdzić pytanie bezpieczeństwa przyciskiem ***Skasuj uprawnienie***.



Rys. 173: Skasowanie uprawnienia

> Zaktualizować nośnik funkcją "Pull to Refresh" w przypadku smartfona lub za pomocą stacji kodującej w przypadku karty, breloka do kluczy, bransoletka lub klucza Combi, aby pomyślnie zakończyć proces.

Skasowanie uprawnienia nie pociąga za sobą kosztu jednostek KeyCredit i następuje natychmiastowo. Jednak do zakończenia procedury kasowania konieczna jest aktualizacja nośnika.

Nie należy korzystać z tej funkcji w ramach reakcji na zgubienie nośników. Uprawnienia można kasować tylko wówczas, gdy nośnik jest fizycznie dostępny. W razie utraty nośnika należy skorzystać z funkcji Dezaktywuj nośnik.

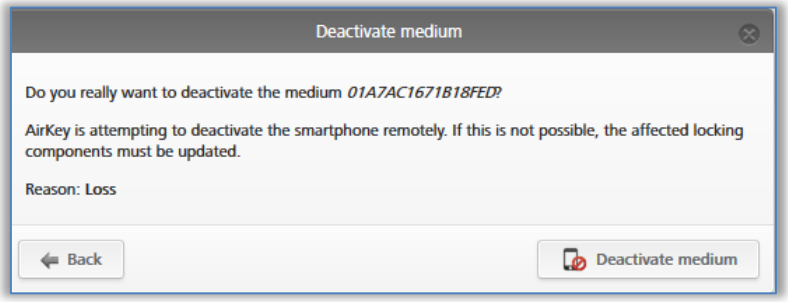
Jeśli zajdzie potrzeba skasowania wszystkich uprawnień nośnika, należy skorzystać z funkcji Wyczyść nośnik.

5.6.17 Dezaktywacja nośnika

Funkcję "Dezaktywuj nośnik" należy stosować wówczas, gdy istnieje zagrożenie bezpieczeństwa i niezbędne jest skasowanie wszystkich uprawnień nośnika, np. w razie zgubienia lub uszkodzenia nośnika.

Rys. 174 Dezaktywacja nośnika

> Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
> Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
> Na liście przeglądu kliknąć żądany nośnik.
> Kliknąć przycisk ***Dezaktywuj nośnik*** ❶.
> Wprowadzić powód dezaktywacji. Po wybraniu opcji "Inny" uaktywni się pole wprowadzania (maks. 50 znaków).
> W razie potrzeby należy wprowadzić dodatkowe informacje (maks. 500 znaków) w polu "Dodatkowe notatki".
> Kliknąć przycisk ***Dalej***.
> Potwierdzić pytanie bezpieczeństwa przyciskiem ***Dezaktywuj nośnik***.



Rys. 175: Dezaktywacja nośnika – pytanie bezpieczeństwa

Dezaktywacja nośnika zostanie potwierdzona komunikatem o pomyślnym zakończeniu procesu.

Wszystkie uprawnienia nośnika zostaną zaznaczone do skasowania. W przypadku kart, breloków do kluczy, bransoletkami i kluczy Combi natychmiast zostanie przygotowany wpis na czarną listę (blacklist) dla wszystkich komponentów zamykających, do których nośnik był uprawniony. W przypadku smartfona wpis na czarną listę zostanie utworzony dopiero wówczas, gdy smartfon będzie niedostępny przez pięć minut. Wpis na czarną listę oznacza, że dla odpowiednich komponentów zamykających zostanie utworzone zadanie konserwacyjne. Odpowiednie komponenty zamykające nie będą mieć aktualnego statusu aż do wykonania aktualizacji.

> Wykonać aktualizację komponentów zamykających, do których nośnik był uprawniony. W ten sposób zadanie konserwacyjne zostanie usunięte z listy i dezaktywowane nośniki nie będą mogły już blokować tych komponentów zamykających.

Nie należy korzystać z tej funkcji do kasowania poszczególnych uprawnień nośnika. Dezaktywacja nośnika jest funkcją, która obejmuje wszystkie uprawnienia nośnika w systemie zamknięć.

Dezaktywacja działa tylko w ramach własnego systemu zamknięć. Jeśli smartfon jest zarejestrowany w kilku systemach zamknięć, status smartfona w pozostałych systemach będzie aktualny i nie zdezaktywowany.

Jeśli osoba zarejestrowała smartfon w kilku systemach zamknięć, w celu kompletnej dezaktywacji smartfona należy poinformować pozostałych administratorów odpowiednich systemów.

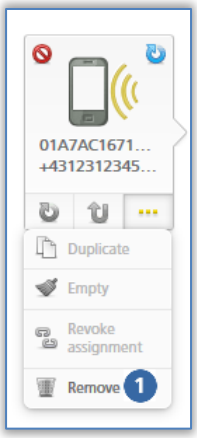
Nośnik nadal pozostaje przypisane do danej osoby. Aby skasować nośnik, należy anulować przypisanie. Bliższe informacje na ten temat można znaleźć w rozdziale Anulowanie przypisania.

5.6.18 Usuwanie dezaktywowanego nośnika

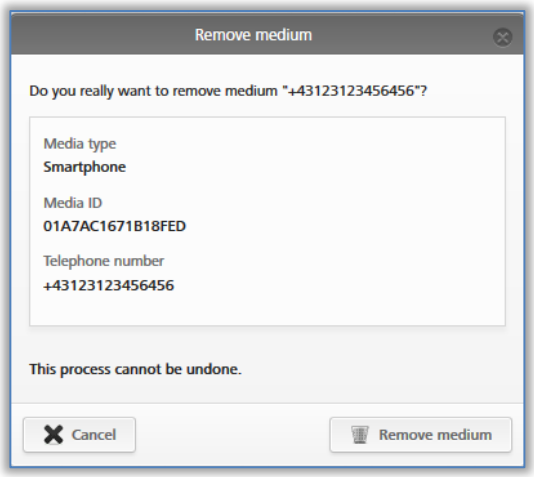
Dezaktywowany nośnik można usunąć z systemu także wówczas, gdy nośnik nie jest dostępny. Dzięki temu zbiór danych podstawowych w module zarządzania online można zminimalizować, np. w przypadku zgubionych, kradzionych lub uszkodzonych nośników.

Usunięcie dezaktywowanego nośnika jest możliwe tylko wówczas, gdy nośnik został całkowicie zdezaktywowany. Oznacza to, że albo nośnik został zaktualizowany, albo do wszystkich komponentów zamykających, wobec których dany nośnik miał uprawnienia, przesłano aktualną czarną listę w ramach aktualizacji. Jeśli powyższe warunki nie są spełnione, usunięcie nie jest możliwe.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć dezaktywowany nośnik, który ma zostać usunięty.
- Poniżej symbolu nośnika kliknąć opcję Więcej i wybrać funkcję ***Usuń*** ❶.
- Potwierdzić pytanie bezpieczeństwa przyciskiem ***Wyjmij nośnik***, aby dezaktywowany aktualny nośnik usunąć z systemu zamknięć.



Rys. 176: Usuwanie dezaktywowanego nośnika



Rys. 177: Usuwanie nośnika – pytanie bezpieczeństwa

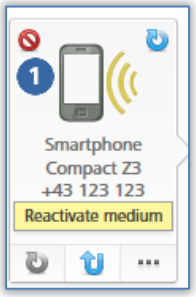
> Pojawi się komunikat o pomyślnym wykonaniu operacji i nośnik nie będzie już uwzględniany w systemie.

Ta operacja nie może być anulowana. Nośniki usunięte w ten sposób nie będą ujęte w zestawieniu w systemie i dlatego zarządzanie nimi nie będzie możliwe.

Nośniki nie przechodzą w ten sposób automatycznie w stan fabryczny.

5.6.19 Reaktywacja nośnika

Dezaktywowany nośnik (można to rozpoznać po czerwonym symbolu przekreślenia ❶ obok nośnika) można reaktywować, gdy będzie on ponownie dostępny.



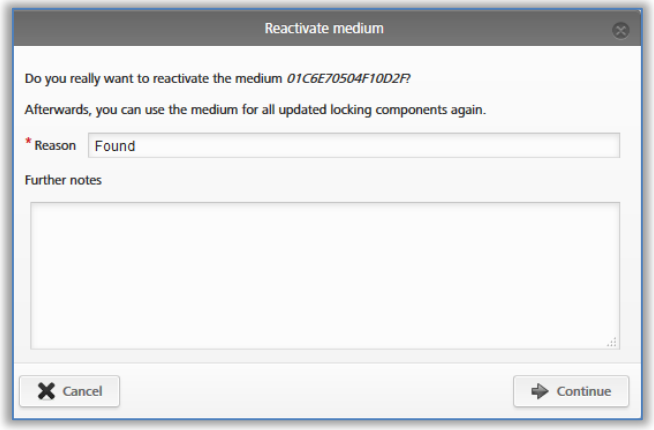
Rys. 178: Reaktywowanie dezaktywowanego nośnika

> Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
> Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
> Na liście przeglądu kliknąć nośnik, dla którego ma nastąpić reaktywacja.
> Kliknąć opcję ***Reaktywuj nośnik*** poniżej symbolu nośnika.

Rys. 179: Reaktywacja nośnika

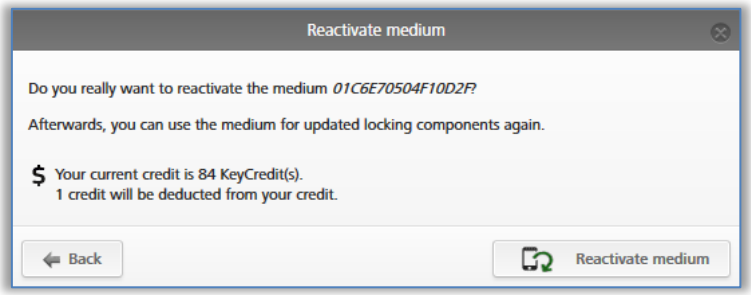
> Wprowadzić powód reaktywacji (mas. 50 znaków) i zdecydować, czy uprawnienia ważne przed dezaktywacją mają być przywrócone.

W razie potrzeby należy wprowadzić dodatkowe informacje (maks. 500 znaków) w polu "Dodatkowe notatki". Te dodatkowe informacje będą dołączone do odpowiedniego wpisu do protokołu.



Rys. 180: Reaktywacja nośnika

> Kliknąć przycisk ***Dalej***.
> Potwierdzić jedno z dwóch pytań bezpieczeństwa (w zależności od wyboru, czy uprawnienia mają zostać przywrócone lub nie) przyciskiem ***Reaktywuj nośnik***.



Rys. 181: Reaktywacja nośnika – przywracanie uprawnień

Reaktywacja nośnika zostanie potwierdzona komunikatem o pomyślnym zakończeniu procesu.

Jeśli dla reaktywowanego nośnika przesłano wpisy czarnej listy na wszystkie uprawnione komponenty zamykające, ponownie powstaną zadania konserwacyjne dla tych komponentów.

Wykonać aktualizację komponentów zamykających, dla których z uwagi na reaktywację nośnika powstało zadanie konserwacyjne. Dopiero gdy wszystkie wpisy na czarną listę zostaną usunięte – tzn. wszystkie odpowiednie komponenty zamykające będą zaktualizowane – odryglowanie wszystkich komponentów zamykających za pomocą nośnika będzie ponownie możliwe.

Reaktywacja jest możliwa tylko w przypadku własnego systemu zamknięć. Jeśli smartfon został dezaktywowany w kilku systemach zamknięć, smartfon nadal będzie nieaktywny w innych systemach i nie będzie mógł w ramach tych systemów odryglować komponentów.

Jeśli osoba zarejestrowała smartfon w kilku systemach zamknięć, w celu

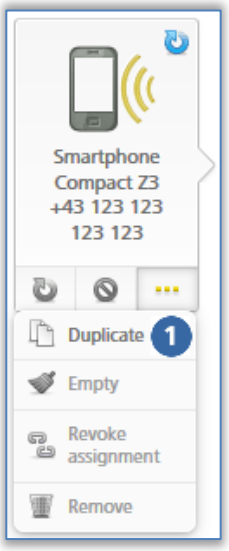
kompletnej reaktywacji należy poinformować pozostałych administratorów wszystkich odpowiednich systemów.

Przywracanie uprawnień spowoduje wyksięgowanie jednostki KeyCredit. Dlatego wymagane jest odpowiednie saldo kredytu.

5.6.20 Kopiowanie nośnika

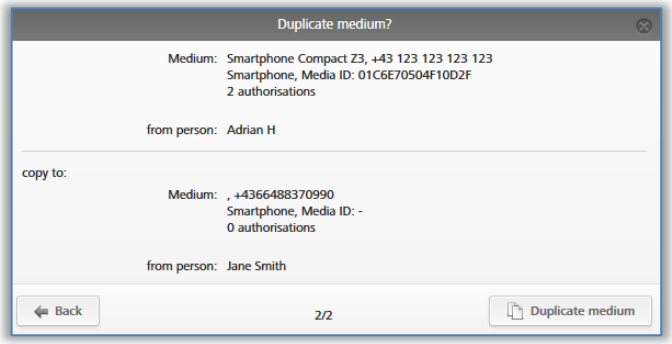
Funkcja kopiowania nośnika służy do przenoszenia istniejących uprawnień nośnika na inny nośnik. Dla tej operacji muszą być spełnione następujące warunki: nośnik źródłowy, który zostanie skopiowany, ma już uprawnienia a nośnik docelowy został już utworzony i przypisany osobie.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć kopiowany nośnik.



Rys. 182: Kopiowanie nośnika

- Kliknąć opcje ***Więcej...*** ❶ → ***Kopiuj***. Otworzy się lista zawierająca wszystkie nośniki przypisane osobie – nośnik przeznaczony do kopiowania nie będzie ujęty na tej liście.
- Wybrać nośnik docelowy i kliknąć przycisk ***Dalej***.
- Zakończyć procedurę przyciskiem ***Duplikuj nośnik***.



Rys. 183: Kopiowanie nośnika

Pomyślne skopiowanie zostanie potwierdzone odpowiednim komunikatem. Widok ekranu przełączy się do okna przeglądu uprawnień nośnika docelowego.

Istniejące uprawnienia na nośniku docelowym zostaną nadpisane.

Aby zakończyć procedurę kopiowania, nośnik docelowy należy przygotować oraz zaktualizować za pomocą funkcji ***Utwórz uprawnienia***. Bliższe informacje na temat przygotowania nośnika znajdują się w rozdziale Potwierdzenie uprawnienia.

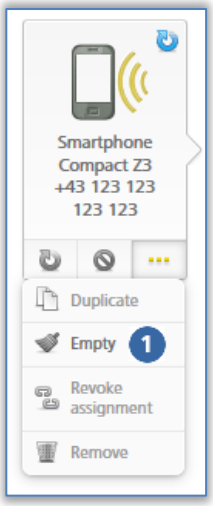
Ta operacja kosztuje jedną jednostkę KeyCredit. Dlatego wymagane jest odpowiednie saldo kredytu.

Jeśli zarządzanie online systemem AirKey obejmuje dużą liczbę osób (patrz Import danych osobowych), których wszystkie uprawnienia są identyczne, wówczas można skorzystać z funkcji "Kopiuj nośnik", aby dużą liczbę nośników z identycznymi uprawnieniami szybko przypisać odpowiednim osobom.

5.6.21 Wyczyszczenie nośnika

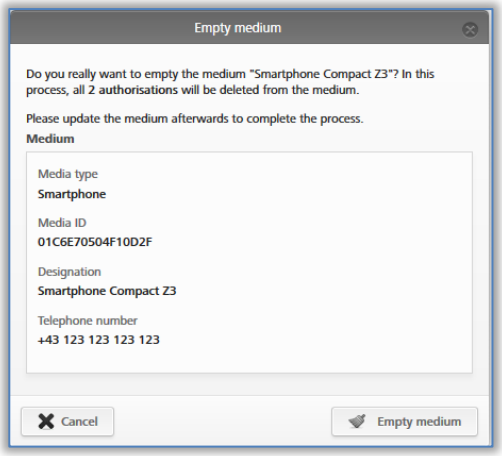
Nośnik należy wyczyścić, gdy zachodzi potrzeba skasowania wszystkich uprawnień z nośnika.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć nośnik, który będzie wyczyszczony.



Rys. 184: Wyczyszczenie nośnika

- Kliknąć opcję ***Więcej...*** ❶ → ***Wyczyść***.
- Zakończyć procedurę przyciskiem ***Wyczyść nośnik***.



Rys. 185: Wyczyszczenie nośnika – pytanie bezpieczeństwa

Wszystkie uprawnienia zostaną zaznaczone w taki sposób, jak do skasowania. Nośnik należy zaktualizować, aby skasowanie uprawnień odniosło skutek.

Usunięcie uprawnień nie generuje kosztu jednostek KeyCredit. Jednak do zakończenia procedury kasowania konieczna jest aktualizacja nośnika.

Nie należy korzystać z tej funkcji w ramach reakcji na zgubienie nośników. Uprawnienia można kasować tylko wówczas, gdy nośnik jest dostępny. W razie utraty nośnika należy skorzystać z funkcji Dezaktywuj nośnik.

Jeśli użytkownik zamierza skasować tylko poszczególne uprawnienia, należy zastosować funkcję Skasuj uprawnienie.

5.6.22 Anulowanie przypisania

Przypisanie należy anulować, gdy osoba nie korzysta już z nośnika.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć nośnik, dla którego nastąpi anulowanie przypisania do osoby.

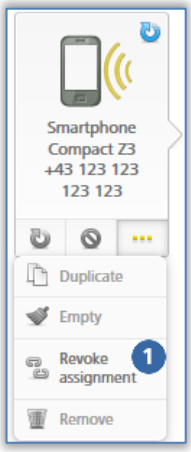
lub

- Na stronie startowej ***Home*** wybrać ikonę ***Osoby***.
- Alternatywnie w menu głównym wybrać opcje ***Nośniki i osoby*** → ***Osoby***.
- Na liście osób kliknąć nazwisko osoby, dla której zostanie anulowane przypisanie nośnika.

Z lewej strony ekranu, poniżej nazwiska osoby zostaną wyświetlone wszystkie nośniki przypisane do tej osoby.

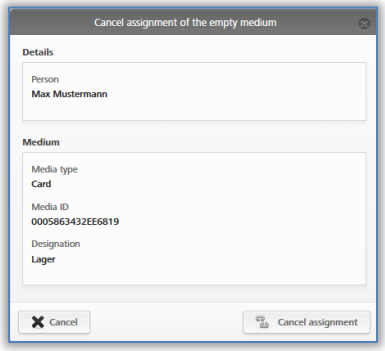
Wybrać nośnik, dla którego nastąpi anulowanie przypisania.

Rys. 186: Przypisane nośniki



Rys. 187: Nośnik – anulowanie przypisania

- Kliknąć opcję ***Więcej...*** ❶ → ***Anuluj przypisanie***, jeśli na nośniku nie ma żadnych uprawnień.
- Potwierdzić pytanie bezpieczeństwa przyciskiem ***Anuluj przypisanie***.



Rys. 188: Anulowanie przypisania bez uprawnień

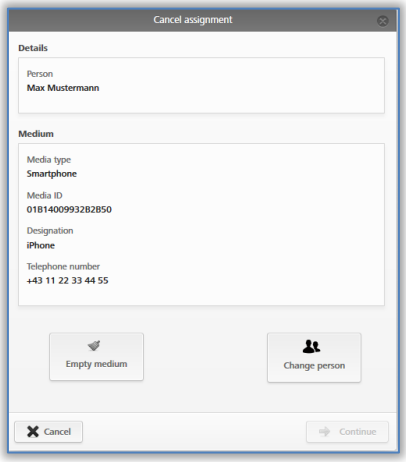
Pomyślne anulowanie przypisania będzie potwierdzone odpowiednim komunikatem. Widok ekranu przełączy się automatycznie na szczegóły danej osoby.

Aby anulowanie przypisania było możliwe w przypadku smartfonów, należy dezaktywować specjalne uprawnienie "uprawnienie do konserwacji".

Jeśli nośnik zawiera uprawnienia, należy je najpierw skasować. Funkcję ***Wyczyść nośnik*** można stosować także w przypadku funkcji ***Anuluj***

przypisanie, aby wyczyścić wszystkie uprawnienia nośnika.

Jeśli na nośniku są jeszcze uprawnienia, podczas wykonywania funkcji ***Anuluj przypisanie*** pojawi się alternatywne okno dialogowe. W tym oknie dialogowym użytkownik ma możliwość wyboru pomiędzy wyczyszczeniem nośnika lub przeniesieniem nośnika na inną osobę.



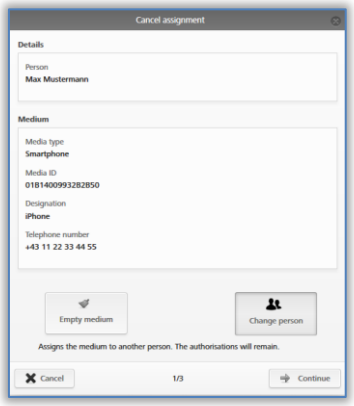
Rys. 189: Anulowanie przypisania z uprawnieniami

Jeśli funkcja ***Wyczyść nośnik*** jest stosowana w związku z funkcją ***Anuluj przypisanie***, po aktualizacji nośnika należy – aby pomyślnie zakończyć proces kasowania uprawnień – należy ponownie wykonać funkcję ***Anuluj przypisanie***.

Aby przenieść nośnik łącznie z uprawnieniami na inna osobę, należy wykonać poniższe czynności:

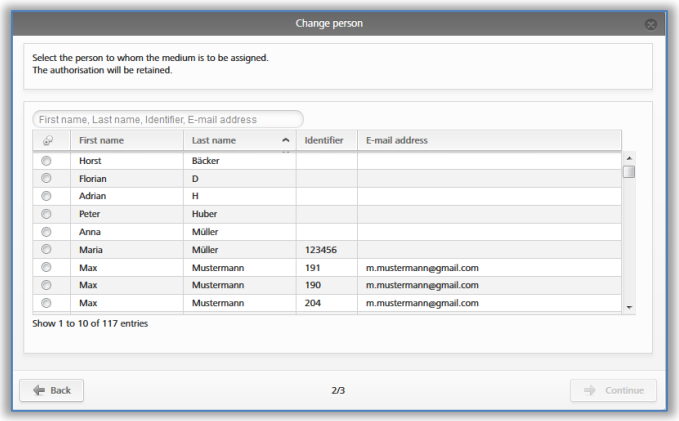
> Kliknąć opcję ***Więcej...*** → ***Anuluj przypisanie***.

> Wybrać opcję ***Zmień osobę*** i potwierdzić przyciskiem ***Dalej***.



Rys. 190: Anulowanie przypisania – zmiana osoby

Zostanie wyświetlona lista wszystkich utworzonych osób. Wybrać żądaną osobę i potwierdzić przyciskiem ***Dalej***.



Rys. 191: Zmiana osoby

Potwierdzić pytanie bezpieczeństwa przyciskiem ***Zmień osobę***, aby pomyślnie zakończyć proces.

Rys. 192: Zmiana osoby

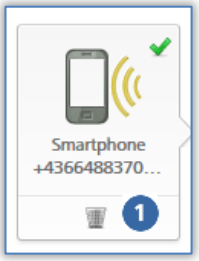
Pomyślne wykonanie operacji będzie potwierdzone odpowiednim komunikatem.

5.6.23 Usuwanie nośnika

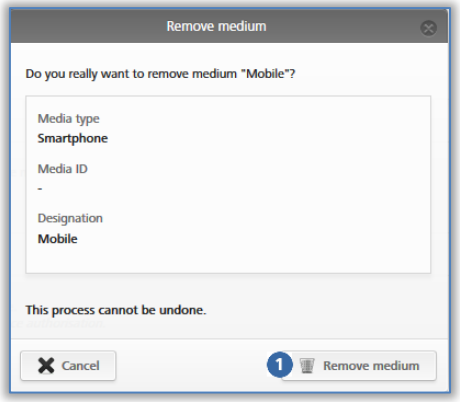
Nośnik należy usunąć, jeśli nie będzie on już wyświetlany ani używany w systemie zamknięć.

Nośnik można usunąć tylko wówczas, gdy zostało anulowane przypisanie do osoby. Bliższe informacje na temat anulowania przypisania znajdują się w rozdziale Anulowanie przypisania.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć nośnik, który będzie usunięty.
- Kliknąć symbol kosza ❶ pod symbolem nośnika.
- Potwierdzić pytanie bezpieczeństwa przyciskiem ***Usuń nośnik*** ❶.



Rys. 193: Usuwanie nośnika – symbol kosza



Rys. 194: Usuwanie nośnika

Jeśli nośnik został całkowicie usunięty, nie będzie widoczny na liście przeglądu nośników. Widok ekranu przełączy się na listę nośników.

Nośnik po usunięciu z systemu będzie ponownie w stanie fabrycznym i można go dodać do innego systemu zamknięć AirKey.

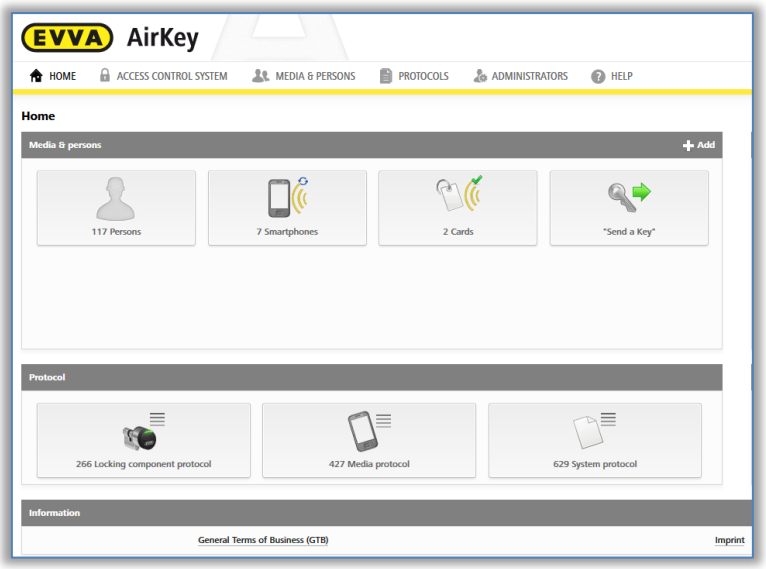
Option

Nośnik bez uprawnień i bez relacji osobowej można usunąć za pomocą stacji kodującej, kładąc na niej nośnik i naciskając w ramach komunikatu o statusie przycisk ***Usuń nośnik z systemu***.

5.7 Protokoły

W menu głównym ***Protokół*** można wyświetlić centralny przegląd wszystkich zdarzeń własnego systemu AirKey. W zależności od ogólnych ustawień dotyczących protokołowania i konserwacji lub relacji osobowych we wpisach do protokołu odbywa się protokołowanie – oprócz udzielonych dostępów i zdarzeń technicznych – także odmowy dostępu (gdy odpowiedni nośnik w momencie weryfikacji miał nieważne, ale zasadniczo istniejące uprawnienie do danego komponentu zamykającego AirKey). Wszystkie przesłane do modułu zarządzania zdarzenia są tam przechowywane bez ograniczeń.

Od czasu do czasu należy załadować widok od nowa, aby zawsze w protokole mieć do dyspozycji najnowsze zdarzenia. Do tego celu służy opcja ***Załaduj widok od nowa***.



Rys. 195: Protokoły

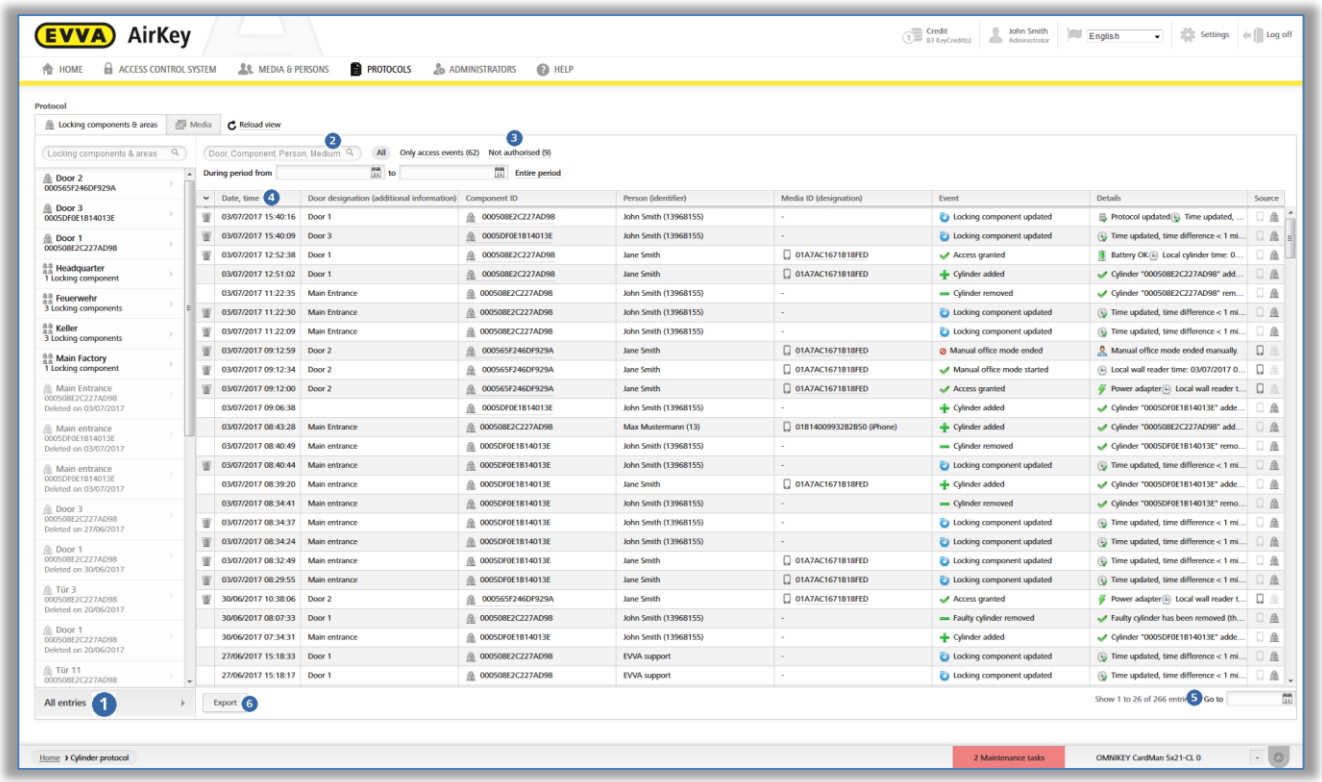
Należy zwrócić szczególną uwagę na fakt, że istniejący system AirKey może podlegać przepisom ustawowym, zwłaszcza w zakresie obowiązków rejestracji/uzyskania zezwoleń wynikających z ustawy o ochronie danych. Stosownie do tego obowiązku firma EVVA Sicherheitssysteme GmbH nie przejmuje żadnej odpowiedzialności i gwarancji w zakresie eksploatacji zgodnej z prawem.

5.7.1 Protokół komponentu zamykającego

- Na stronie startowej ***Home*** wybrać ikonę ***Protokół komponentu zamykającego***.
- Alternatywnie wybrać w menu głównym opcje ***Protokoły*** → ***Komponenty zamykające & strefy***.

Wyświetlona lista zawiera wpisy dotyczące komponentów zamykających lub stref.

- W razie potrzeby wybrać z lewej kolumny poszczególne komponenty zamykające lub strefy, dla których ma zostać wyświetlony protokół. Aby ponownie wyświetlić wszystkie komponenty zamykające i strefy, należy kliknąć opcję ***Wszystkie wpisy*** ❶ z lewej strony, na dole ekranu.
- W przypadku szczegółowego wyszukiwania wpisów wprowadzić co najmniej 3 znaki w polu wyszukiwania ❷.
- Dodatkowo można aktywować filtr ❸, klikając żądany link (np. "Brak uprawnień"). W tym przypadku nastąpi wyświetlenie tylko tych wpisów, dla których zastosowano odmowę dostępu.
- Lista jest standardowo posortowana według daty i godziny ❹ (najnowsze wpisy są na górze). Klikając nagłówek kolumny "Data, godzina", można zmienić kierunek sortowania. Sortowanie według innych nagłówków kolumn w tej tabeli nie jest możliwe.



Rys. 196: Protokół komponentów zamykających i stref

- Jeśli lista zawiera bardzo duża liczbę wpisów, można użyć pola ***Idź do*** ❺ znajdującego się w prawej, dolnej części ekranu, aby szybko przejść do określonego dnia kalendarzowego.
- Należy użyć przycisku ***Eksportuj*** ❻ w lewej, dolnej części ekranu, jeśli ma zostać wyeksportowany cały protokół do pliku CSV. Plik można przetwarzać niezależnie od Modułu zarządzania online systemu AirKey.

W protokole zawarte są wszystkie niezbędne informacje, takie jak data i godzina, oznaczenie drzwi (informacja dodatkowa), ID komponentu, osoba (identyfikator), ID nośnika (oznaczenie) oraz zdarzenie. Ponadto w kolumnie "Szczegóły" są wyświetlane bliższe informacje dotyczące zdarzenia.

Kolumna "Źródło" wskazuje, czy wpis do protokołu pochodzi z nośnika i/lub komponentu zamykającego.

Od czasu do czasu należy załadować widok od nowa, aby w protokole mieć do dyspozycji najnowsze zdarzenia. Do tego celu służy opcja ***Załaduj widok od nowa***.

Ustawienia protokołowania służą do ograniczenia protokołowania relacji osobowych we wpisach do protokołu zgodnie z przepisami z zakresu ochrony danych. Rodzaj relacji osobowej we wpisach do protokołu dla komponentów zamykających można określić dla nowo dodawanych komponentów w ustawieniach wartości domyślnych dla protokołowania lub dla poszczególnych komponentów w sekcji szczegółów komponentu zamykającego.

Tylko za pomocą regularnej aktualizacji komponentów zamykających można zapewnić, że wszystkie wpisy z protokołu komponentów zamykających zostają przesłane do modułu zarządzania online. Zalecane interwały aktualizacji zależą od intensywności użytkowania komponentu zamykającego. Należy uwzględnić parametry i limity komponentów AirKey.

Odmowa dostępu jest protokołowana tylko wówczas, gdy nośnik zawiera uprawnienie do komponentu zamykającego, ale nie było ono ważne w momencie dostępu (np. okres obowiązywania uprawnienia upłynął lub uprawnienie jest ważne tylko w określonym przedziale czasu).

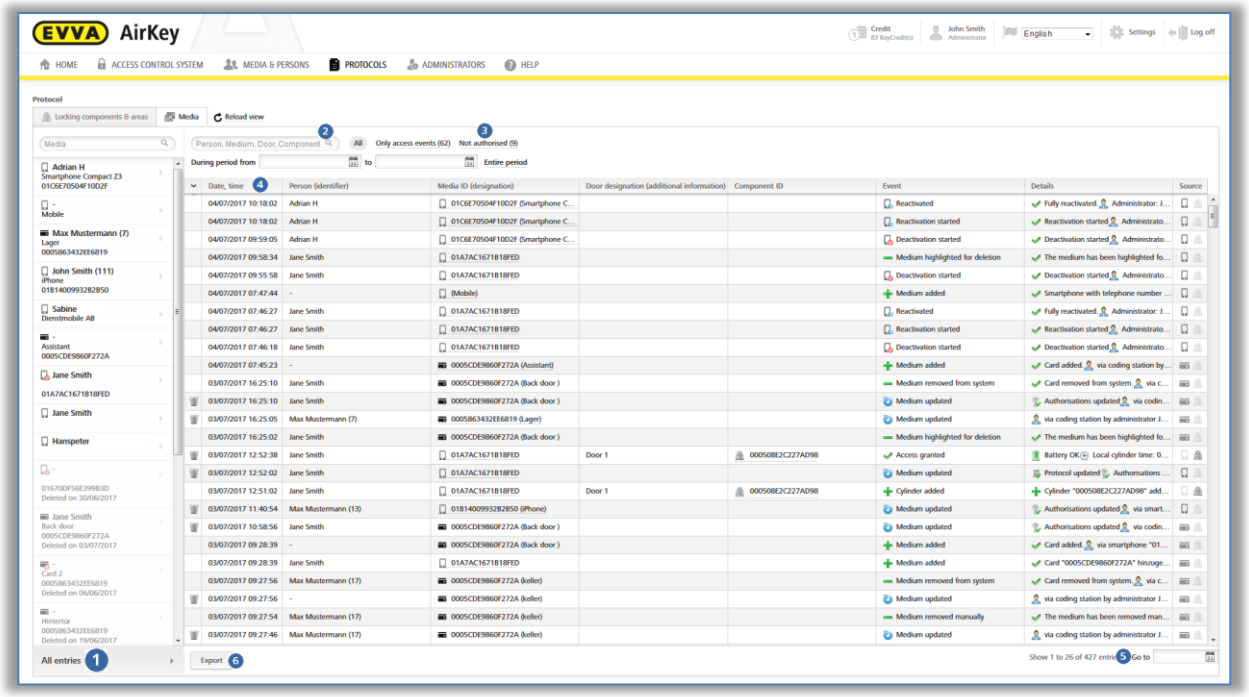
Wskazywany stan baterii w kolumnie "Szczegóły" to zawsze stan baterii komponentu zamykającego AirKey (wkładki), a nie stan baterii smartfona.

Jeśli w przypadku komponentów zamykających protokołowanie jest ograniczone do zdefiniowanego okresu, zdarzenia dostępu są mimo to protokołowane po upływie tego okresu. W takim przypadku następuje tylko anonimizacja relacji osobowych.

5.7.2 Protokół nośnika

> Na stronie startowej ***Home*** wybrać ikonę ***Protokół nośników***.

> Alternatywnie wybrać w menu głównym opcje ***Protokoły*** → ***Nośniki***.



Rys. 197: Protokół nośnika

Zostanie wyświetlony przegląd wszystkich wpisów nośników.

> W razie potrzeby wybrać poszczególne nośniki, dla których ma zostać wyświetlony protokół, z lewej kolumny. Aby ponownie wyświetlić wszystkie nośniki, należy kliknąć ***Wszystkie wpisy*** ❶ na dole ekranu, z lewej strony.

- W przypadku szczegółowego wyszukiwania wpisów wprowadzić co najmniej 3 znaki w polu wyszukiwania ❷.
- Włączyć filtr, np. "Brak uprawnień" ❸. W tym przypadku nastąpi wyświetlenie tych wpisów, dla których zastosowano odmowę dostępu.
- Posortować listę według daty i godziny ❹.
- Skorzystać z pola ***Idź do*** ❺ z prawej strony, na dole ekranu, aby szybko przejść do określonego dnia w przypadku obszernej listy.
- Należy użyć przycisku ***Eksportuj*** ❻ w lewej, dolnej części ekranu, jeśli ma zostać wyeksportowany cały protokół nośnika do pliku CSV. Plik można przetwarzać niezależnie od Modułu zarządzania online systemu AirKey.

W protokole są ujęte wszystkie niezbędne informacje, takie jak data i godzina, osoba (identyfikator), ID nośnika (oznaczenie), oznaczenie drzwi (informacja dodatkowa), ID komponentu oraz zdarzenie. Ponadto w kolumnie "Szczegóły" są wyświetlane dokładniejsze informacje dotyczące zdarzenia.

Kolumna "Źródło" wskazuje, czy wpis do protokołu pochodzi z nośnika i/lub komponentu zamykającego.

Ustawienia protokołowania służą do ograniczenia protokołowania relacji osobowych we wpisach do protokołu zgodnie z przepisami z zakresu ochrony danych. Rodzaj relacji osobowej we wpisach do protokołu dla komponentów zamykających można określić dla nowo dodawanych komponentów w ustawieniach lub dla poszczególnych komponentów w sekcji szczegółów komponentu zamykającego.

Wpisy do protokołu określonego nośnika można także wyświetlić za pośrednictwem widoku danego nośnika. W tym celu należy wybrać żądany nośnik z listy nośników i przejść do zakładki ***Protokół***.

Odmowa dostępu jest protokołowana tylko wówczas, gdy nośnik zawiera uprawnienie do komponentu zamykającego, ale nie było ono ważne w momencie dostępu (np. okres obowiązywania uprawnienia upłynął lub uprawnienie jest ważne tylko w określonym przedziale czasu).

Wskazywany stan baterii w kolumnie "Szczegóły" to zawsze stan baterii komponentu zamykającego AirKey (wkładki), a nie stan baterii smartfona.

Jeśli w przypadku komponentów zamykających protokołowanie jest ograniczone do zdefiniowanego okresu, zdarzenia dostępu są mimo to protokołowane po upływie tego okresu. W takim przypadku następuje tylko anonimizacja relacji osobowych.

W przypadku protokołu komponentu zamykającego i protokołu nośnika obowiązuje zasada, że wpisy do protokołu z relacją osobową można również później zanonimizować ze względu na wymagania prawne z zakresu ochrony danych. Wpisy do protokołu o krytycznym znaczeniu dla ochrony danych (np. dostępy) są w pierwszej kolumnie wyróżnione symbolem kosza.

Aby anonimizować relacje osobowe we wpisach do protokołu, należy wykonać następujące czynności:

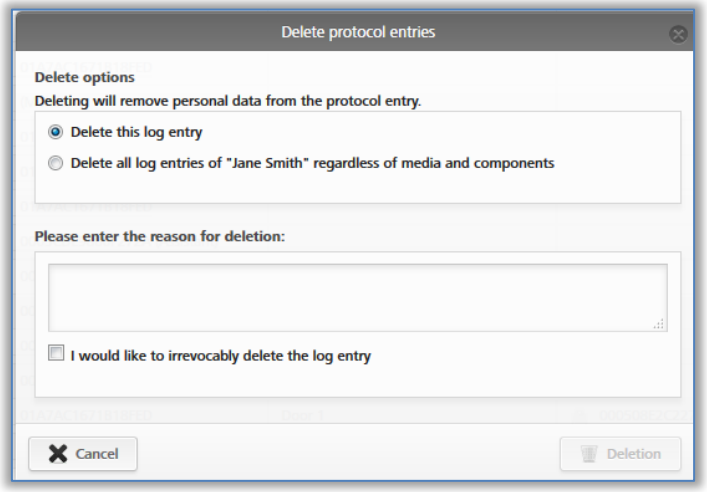
> Wyszukać wpis do protokołu, który będzie anonimizowany i kliknąć symbol kosza umieszczony w pierwszej kolumnie.

> Wyświetli się pytanie, czy należy usunąć tylko ten wpis lub wszystkie wpisy dotyczące tej osoby. Wybrać żądaną opcję.

> Wprowadzić powód skasowania wpisu do protokołu.

> Umieścić zaznaczenie w polu wyboru ***Chcę nieodwołalnie usunąć wpis/wpisy do protokołu***.

> Aby zakończyć procedurę, należy potwierdzić przyciskiem ***Usuń***.



Rys. 198: Usuwanie wpisów do protokołu

Wpis do protokołu nie został zupełnie usunięty, ale tylko relacja osobowa. W ten sposób wykonano anonimizację wpisu do protokołu. Ta operacja nie może być anulowana. Należy korzystać z tej funkcji z dużą ostrożnością.

Usunięcie wpisu do protokołu jest ujęte w liście protokołu systemowego.

5.7.3 Protokół systemowy

> Na stronie startowej ***Home*** wybrać ikonę ***Protokół systemowy***.

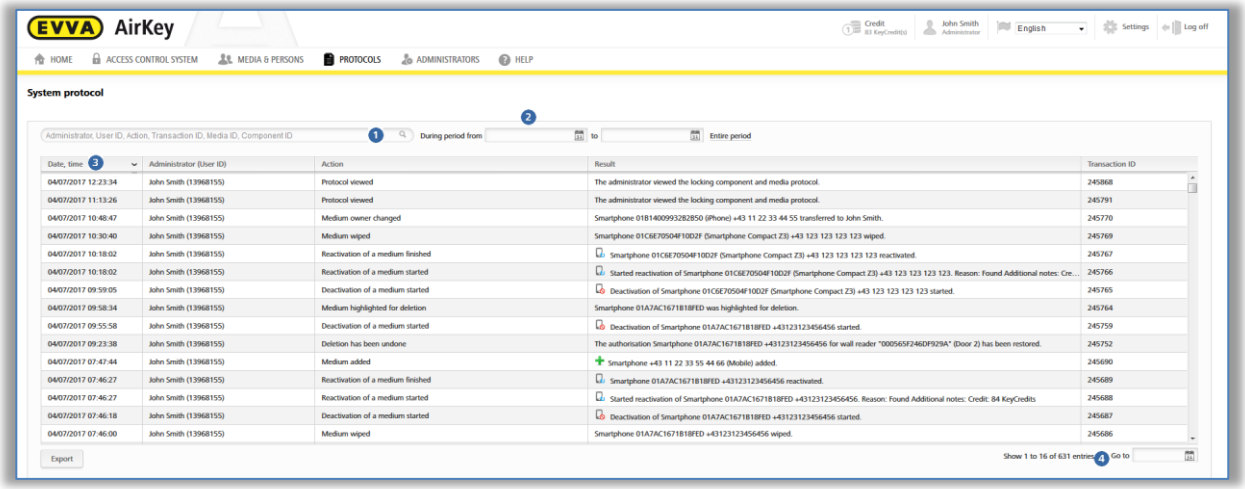
> Alternatywnie wybrać w menu głównym opcje ***Protokoły*** → ***System***.

Zostanie wyświetlony przegląd wszystkich działań, które zostały wykonane przez administratorów.

> W polu wyszukiwania ❶ można wyszukiwać według administratora, identyfikatora użytkownika, wykonanego działania, ID operacji, ID nośnika lub ID komponentu. Wprowadzić wybrany okres ❷ i wybrać kolumnę, według której będzie wykonane sortowanie ❸.

> W polu ***Idź do*** ❹ wprowadzić datę, aby przejść bezpośrednio do protokołu systemowego z określonego dnia. Jeśli nie ma żadnych wpisów dla wybranej daty, zostanie wybrany kolejny, następny wpis.

> Należy użyć przycisku ***Eksportuj*** w lewej, dolnej części ekranu, jeśli ma zostać wyeksportowany cały protokół systemowy do pliku CSV. Plik można przetwarzać niezależnie od Modułu zarządzania online systemu AirKey.



Rys. 199: Protokół systemowy

Nie można usunąć żadnych wpisów z protokołu systemowego.

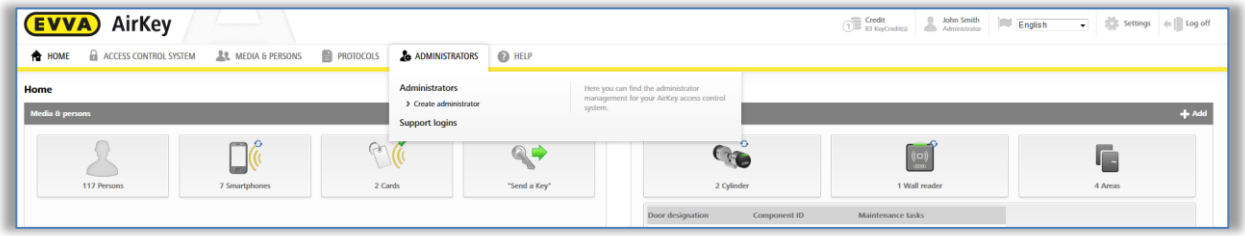
5.8 Dostęp do pomocy technicznej

Jeśli potrzebna jest pomoc techniczna w zakresie funkcjonowania systemu AirKey, można utworzyć ograniczone czasowo konto administratora, służące jako dostęp do pomocy technicznej. Za pomocą dostępu do pomocy technicznej użytkownik możliwe jest wyświetlenie kompletnych danych systemu zamknięć.

Użytkownik tego dostępu dysponuje przez okres udostępnienia identycznymi uprawnieniami co właściwy administrator systemu.

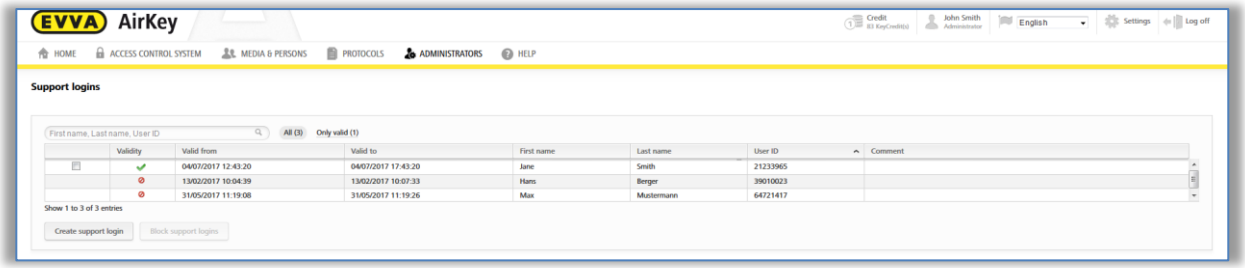
5.8.1 Tworzenie dostępu do pomocy technicznej

> Wybrać w menu głównym opcje ***Administratorzy*** → ***Dostęp do pomocy technicznej***.



Rys. 200: Dostęp do pomocy technicznej

Jeśli został już utworzony dostęp do pomocy technicznej, zostanie od wyświetlony na liście.



Rys. 201: Lista dostępu do pomocy technicznej

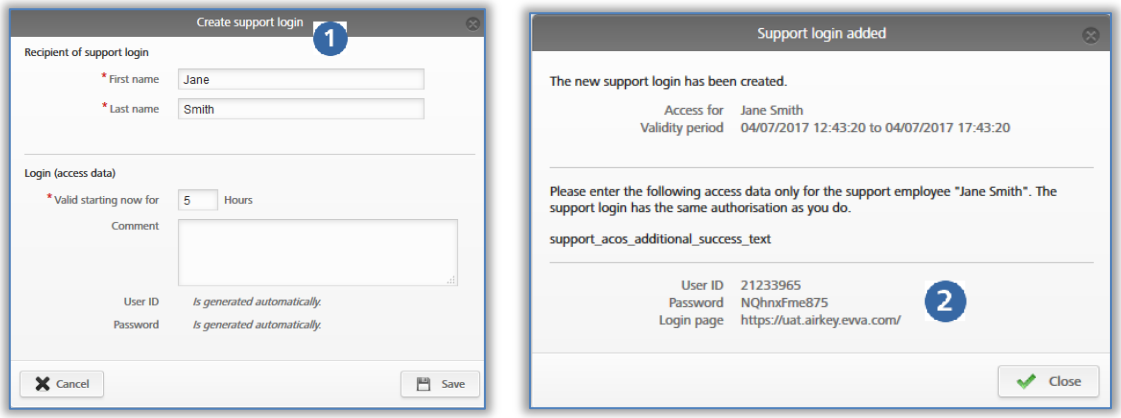
> Kliknąć przycisk ***Tworzenie dostępu do pomocy technicznej***.

> Wypełnić formularz ❶.
Pola oznaczone gwiazdką (*) są obowiązkowe.

Okres obowiązywania dostępu powinien wynosić od 1 do maks. 24 godzin.

> Kliknąć przycisk ***Zapisz***.

Zostanie utworzony dostęp do pomocy technicznej, a także identyfikator z hasłem ❷.



Rys. 202: Tworzenie dostępu do pomocy technicznej

Hasła nie można ponownie wyświetlić po zamknięciu okna dialogowego.

Użytkownik we własnym interesie powinien w bezpieczny sposób zachować dane logowania.

> ***Zamknąć*** okno dialogowe "Tworzenie zezwolenia do pomocy technicznej", gdy dane zostały przekazane partnerowi ds. pomocy technicznej.

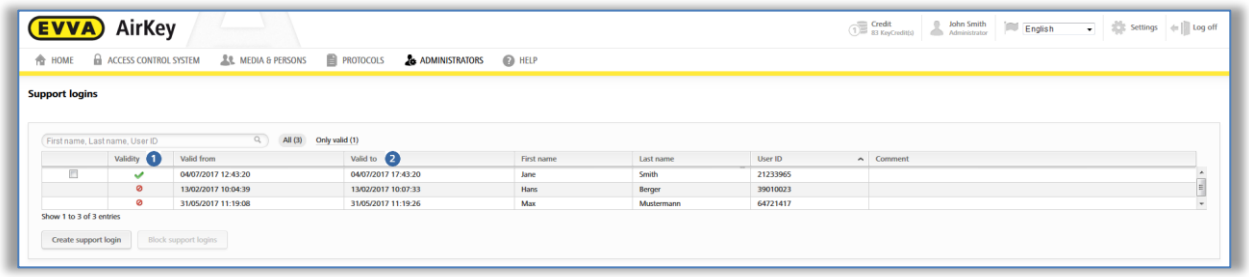
5.8.2 Blokowanie dostępu do pomocy technicznej

Dostęp do pomocy technicznej automatycznie kończy się po upływie zdefiniowanego okresu obowiązywania. Można jednak zakończyć działanie dostępu wcześniej poprzez funkcję ***Blokowanie dostępu do pomocy technicznej***.

Aby wcześniej zablokować funkcję dostępu do pomocy technicznej, należy wykonać poniższą procedurę:

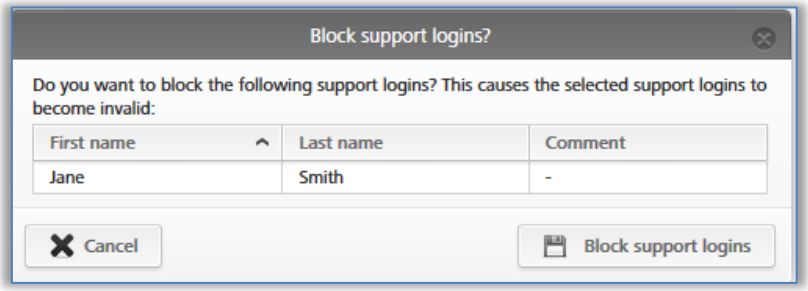
> Wybrać w menu głównym opcje ***Administratorzy*** → ***Dostęp do pomocy technicznej***.

Na liście dostępów do pomocy technicznej można zobaczyć, czy istnieje aktualnie ważny dostęp ❶ i jaki jest jego okres obowiązywania ❷.



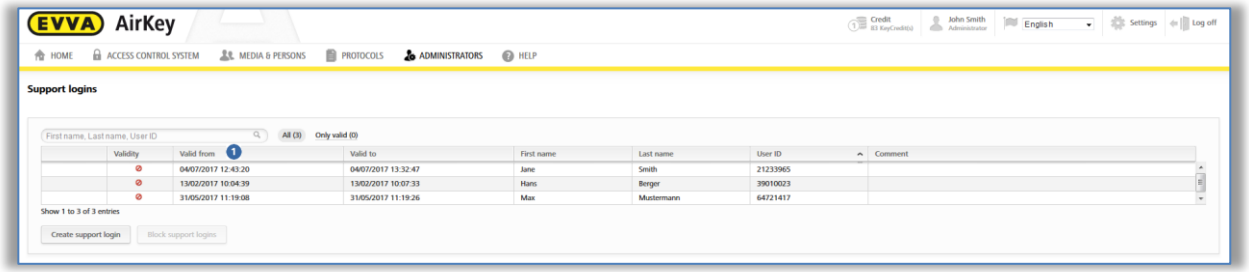
Rys. 203: Przegląd dostępu do pomocy technicznej

> Wybrać odbiorcę dostępu do pomocy technicznej, w przypadku którego zostanie zakończony dostęp.
> Kliknąć przycisk ***Blokowanie dostępu do pomocy technicznej***.
> Potwierdzić pytanie bezpieczeństwa przyciskiem ***Blokowanie dostępu do pomocy technicznej***.



Rys. 204: Blokowanie dostępu do pomocy technicznej

Na liście dostępów do pomocy technicznej można rozpoznać po symbolu w kolumnie "Ważne" ❶, że nastąpiło zablokowanie dostępu.



Rys. 205: Ważność dostępu do pomocy technicznej

Zarówno czynności wykonane przez odbiorcę dostępu do pomocy technicznej, jak i utworzenie lub zablokowanie tego dostępu zostaną odpowiednio ujęte w protokołach.

5.9 Pomoc

Obszerne materiały pomocowe można znaleźć w menu głównym ***Pomoc*** lub na stronie internetowej dotyczącej produktów AirKey firmy EVVA, pod adresem https://www.evva.com/pl/airkey/website/. Można także skorzystać ze wsparcia świadczonego przez wyspecjalizowanych dystrybutorów firmy EVVA.

6 Aplikacja AirKey

W tym rozdziale zawarto przegląd funkcji, które można wykonać przy użyciu smartfona w ramach aplikacji AirKey.

Aby użyć aplikacji AirKey na smartfonie, powinien on spełnić poniższe warunki:

- Smartfon powinien spełniać wymagania systemowe dla aplikacji AirKey.
- Aplikacja AirKey została pomyślnie zainstalowana na smartfonie.
- Dostępne jest aktywne połączenie z Internetem.

Stosowanie rozwiązań optymalizujących działanie aplikacji, np. służących do oszczędzania baterii, może wpłynąć na funkcjonalność aplikacji. Możliwe skutki to: Proces odryglowania trwa dłużej, odryglowanie w tle działa niestabilnie itp.

6.1 Komponenty Bluetooth

W tym punkcie menu można uzyskać listę zawierającą wszystkie komponenty zamykające Bluetooth znajdujące się w zasięgu. Za pomocą tej strony można np. połączyć się z komponentem, zablokować komponenty Bluetooth lub za pomocą symbolu w prawej, górnej części ekranu nawiązać połączenie z komponentem NFC.

Oznaczenie komponentu Bluetooth będzie prawidłowo wyświetlane dopiero po aktualizacji smartfona, tzn. wskazanie oznaczenia komponentu zamykającego w aplikacji AirKey nie zmienia się automatycznie po dopasowaniu w Module zarządzania online systemu AirKey.

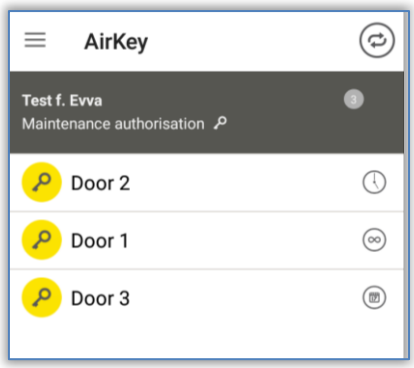
Od wersji systemu Android 6 firma Google wymaga, aby dla potrzeb rozpoznawania komponentów Bluetooth przyznane zostało na smartfonie uprawnienie do ustalania lokalizacji.

6.2 Rejestracja smartfona: patrz rozdział 4.9

6.3 Uprawnienia

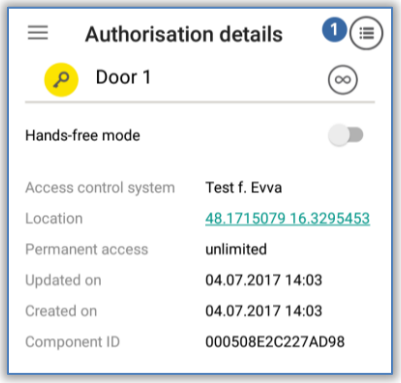
Jeśli smartfon jest już zarejestrowany w systemie AirKey i uprawnienia zostały już utworzone i potwierdzone w Module zarządzania online systemu AirKey, użytkownik ma w każdym momencie możliwość wglądu w uprawnienia smartfona.

- Uruchomić aplikację AirKey.
- W menu wybrać opcję ***Uprawnienia***.



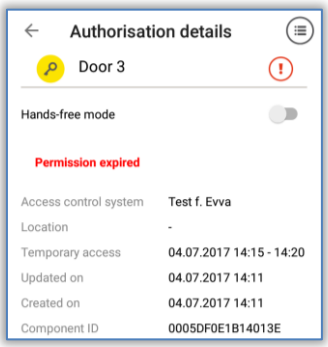
Rys. 206: Aplikacja AirKey – przegląd uprawnień

- Stuknąć jedno z uprawnień, aby wyświetlić szczegóły uprawnienia. Dane lokalizacyjne (współrzędne GPS lub adres) będą przedstawiane w formie linku. Po naciśnięciu linku nastąpi automatyczne przejście do operatora karty, który jest ustawiony jako standardowy na określonym smartfonie.
- W szczegółach uprawnień można także indywidualnie aktywować tryb "Hands free" dla każdego uprawnienia. W takiej sytuacji wymagane jest, aby tryb "Hands free" został aktywowany w ustawieniach aplikacji.



Rys. 207: Aplikacja AirKey – szczegóły uprawnienia

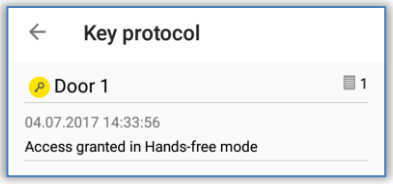
Jeśli ważność uprawnienia dostępowego już upłynęła, będzie to odpowiednio wskazane na ekranie.



Rys. 208: Upłynął okres ważności uprawnienia

Jeśli smartfon jest uprawniony do wyświetlania danych z protokołów (patrz rozdział Dane z protokołów w aplikacji AirKey), w szczegółach uprawnienia ❶ zostanie wyświetlony protokół przynależny do wybranego uprawnie-

nia.



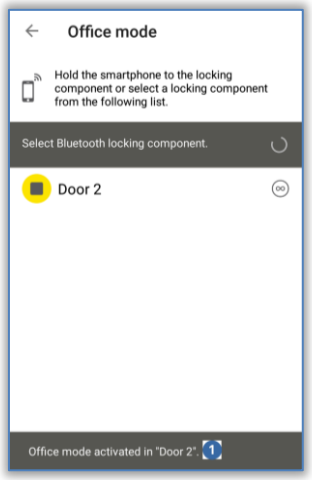
Rys. 209: Dane z protokołu określonego uprawnienia

6.4 Zadania konserwacyjne: patrz rozdział 6.12

6.5 Stałe otwarcie

W przypadku stałego otwarcia wymagane jest, aby w Module zarządzania online systemu AirKey było aktywowane ręczne stałe otwarcie dla komponentów zamykających AirKey (patrz rozdział Edytuj komponent zamykający) zarówno dla komponentów Bluetooth, jak i NFC.

- W aplikacji AirKey wybrać menu ***Stałe otwarcie***.
- Z wyświetlonej listy wybrać komponent zamykający Bluetooth lub przytrzymać smartfon przy komponencie zamykającym NFC.
- Komponent optycznie i akustycznie zasygnalizuje blokowanie.
- Pojawi się komunikat o pomyślnym wykonaniu operacji ❶.



Rys. 210: Stałe otwarcie – komunikat

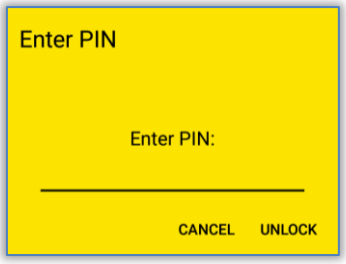
Aktywowanie stałego otwarcia dla komponentów zamykających i nośników zwiększa pobór prądu komponentów. Stałe otwarcie należy aktywować tylko w przypadku tych komponentów zamykających i nośników, które faktycznie będą korzystać z tej funkcji.

6.6 Wprowadzenie kodu PIN

Aktywny kod PIN można zapisać w pamięci pośredniej aplikacji AirKey na określony czas, korzystając z funkcji ***Wprowadź PIN***.

- Otworzyć menu w aplikacji AirKey i kliknąć opcję Wprowadź PIN.

> Wprowadzić prawidłowy kod PIN i nacisnąć opcję ***Odblokuj.***



Rys. 211: Aplikacja AirKey – wprowadzanie kodu PIN

Kod PIN będzie zapisany w pamięci pośredniej aż do momentu, gdy aplikacja AirKey zostanie zamknięta, przełączona do działania w tle lub zostanie aktywowana blokada ekranu. W ten sposób można blokować komponenty zamykające bez ponownego wpisywania kodu PIN.

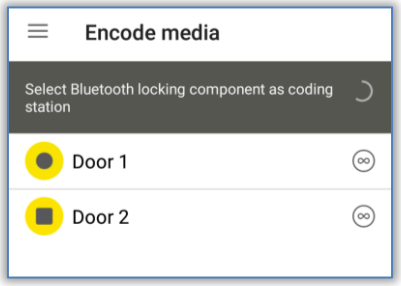
Kod PIN będzie także zapamiętany w pamięci pośredniej, jeśli jest wymagany do pierwszego odblokowania komponentu zamykającego. Podczas kolejnego odblokowania komponentu zamykającego (tego samego lub innego) kod PIN nie będzie już wymagany. To obowiązuje aż do momentu, gdy aplikacja AirKey zostanie zamknięta, przełączona do działania w tle lub zostanie aktywowana blokada ekranu.

6.7 Kodowanie nośników

Ta funkcja aplikacji AirKey umożliwia aktualizowanie nośników dostępu (z wyjątkiem smartfonów) poprzez komponenty zamykające Bluetooth (wkładki, czytniki naścienne).

> W menu AirKey wybrać opcję ***Koduj nośniki***.

> Z listy wyświetlonych komponentów zamykających Bluetooth wybrać te, poprzez które ma nastąpić aktualizacja nośnika.



Rys. 212: Kodowanie nośników – lista wyboru komponentów Bluetooth

> Przytrzymać nośnik przeznaczony do aktualizacji przy komponencie zamykającym AirKey.

Rys. 213: Kodowanie nośników

> Teraz należy postępować zgodnie z instrukcjami zawartymi w rozdziale Dodawanie kart, breloków do kluczy i kluczy Combi za pomocą smartfona.

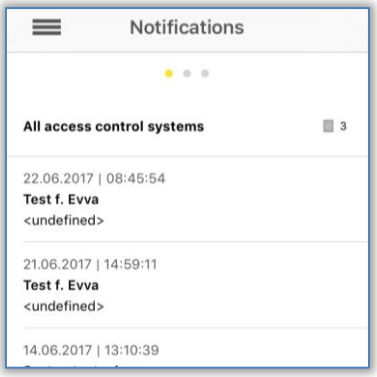
W przypadki funkcji "Koduj nośniki" procedurę należy rozpocząć ręcznie, przy wkładce, a nie za pomocą nośnika (karty, breloka do kluczy, bransoletki lub klucza Combi). W przeciwnym razie nastąpiłby normalny proces odryglowania zamiast nawiązania komunikacji ze smartfonem.

W przypadku komponentów zamykających zasilanych bateryjnie proces aktualizacji powoduje zużycie energii, co skraca okres użytkowania baterii. Jeśli wiele nośników ma zostać objętych aktualizacją, zaleca się skorzystanie ze stacji kodującej AirKey, smartfona z obsługą NFC lub z czytnika naściennego.

Tryb "Hands free" musi być dezaktywowany na smartfonie, aby możliwe było wykonanie funkcji "Koduj nośniki".

6.8 Protokół uprawnień

W menu głównym aplikacji AirKey wybrać punkt ***Protokół uprawnień***, aby uzyskać protokół dotyczący zmian uprawnień, przeprowadzonych przez administratora systemu zamknięć AirKey dla smartfona określonego użytkownika.
To protokołowanie zachodzi zawsze, niezależnie od różnych ustawień w Module zarządzania online systemu AirKey oraz aplikacji AirKey.



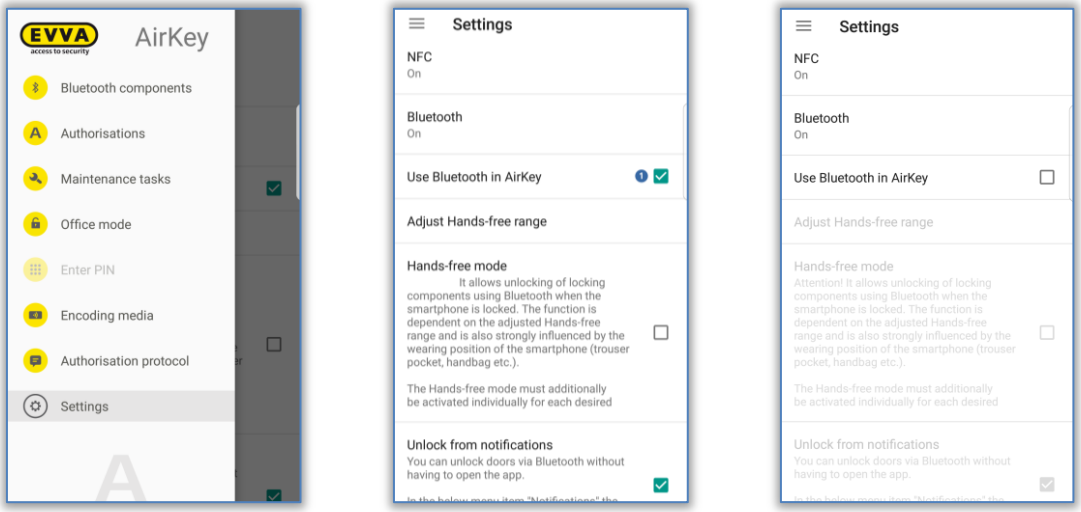
Rys. 214: Protokół uprawnień

6.9 Ustawienia aplikacji mobilnej AirKey

6.9.1 Ustawienia aplikacji AirKey na smartfonach Android

W punkcie menu ***Ustawienia*** aplikacji AirKey są przedstawione podstawowe informacje na temat danego smarftona Android. Można tu np. zobaczyć, czy funkcja NFC i Bluetooth jest aktywna. Stuknąć jedną z dwóch pozycji, aby przejść do ustawień urządzenia na smartfonie. Następnie należy zdecydować, czy funkcja Bluetooth ma być używana w ramach systemu AirKey. Wówczas należy aktywować odpowiednią opcję "Zastosuj Bluetooth" ❶.

W takim przypadku można także skonfigurować kolejne ustawienia następcze ("Ustawianie zasięgu trybu Hands-free", "Tryb Hands free" i "Odblokowanie z powiadomień"). Wówczas strona startowa podczas otwierania aplikacji AirKey to "Komponenty Bluetooth".



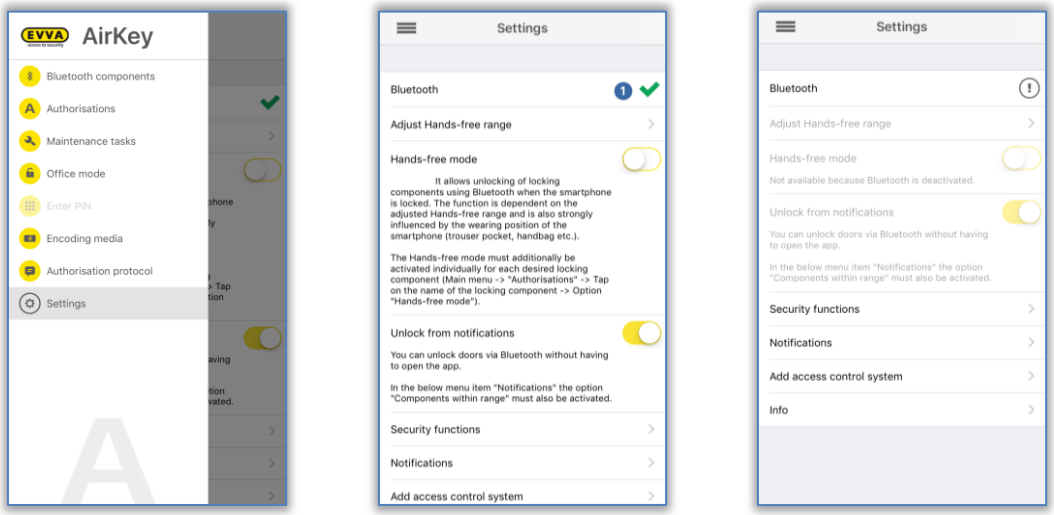
Rys. 215: Smartfon Android z funkcją Bluetooth – menu główne / opcja "Zastosuj Bluetooth" aktywna / opcja Bluetooth dezaktywowana

Jeśli opcja "Zastosuj Bluetooth" zostanie zdezaktywowana, trzy wyżej wspomniane ustawienia następcze będą automatycznie dezaktywowane a wszystkie inne funkcje zależne od Bluetooth z menu głównego ("Komponenty Bluetooth", "Stałe otwarcie" i "Koduj nośniki") będą opatrzone wskazówką "Funkcja Bluetooth jest dezaktywowana". W takiej sytuacji smartfon może komunikować się z komponentami zamykającymi poprzez połączenie NFC.

Jeśli smartfon Android jest starszy i obsługuje NFC, ale nie obsługuje funkcji Bluetooth, wszystkie funkcje i ustawienia zależne od Bluetooth będą wygaszone.

6.9.2 Ustawienia aplikacji AirKey na iPhone'ach

W punkcie menu ***Ustawienia*** aplikacji AirKey są przedstawione podstawowe informacje na temat danego iPhone'a. Można tu np. zobaczyć, czy funkcja Bluetooth jest aktywna. W takim przypadku można także skonfigurować kolejne ustawienia następcze ("Ustawianie zasięgu trybu Hands-free", "Tryb Hands free" i "Odblokowanie z powiadomień").



Rys. 216: iPhone (tylko z Bluetooth) – manu główne / ustawienia bez funkcji zależnych od NFC / opcja Bluetooth dezaktywowana

Pozycja "Bluetooth" w ustawienia aplikacji AirKey wskazuje tylko, czy funkcja Bluetooth jest aktywna lub nie. Mimo to można stuknąć pozycję "Bluetooth", aby przejść do ustawień Bluetooth w ustawieniach urządzenia.

Jeśli Bluetooth zostanie dezaktywowany w ustawieniach iPhone'a, odryglowanie komponentów zamykających NIE BĘDZIE MOŻLIWE!

Nieaktywna funkcja Bluetooth będzie odpowiednio wskazana w ustawieniach aplikacji AirKey i trzy zależne od tej funkcji ustawienia następcze będą automatycznie dezaktywowane, dokładnie tak jak wszystkie pozostałe funkcje zależne od Bluetooth z menu głównego ("Komponenty Bluetooth", "Stałe otwarcie" i "Koduj nośniki").

6.9.3 Ustawianie zasięgu trybu Hands-free

Po wybraniu funkcji "Ustaw zasięg trybu Hands free" nastąpi przejście do podmenu. Tutaj można określić, dla którego typu komponentu zamykającego należy ustawić zasięg lub czy zasięgi (dla wszystkich komponentów zamykających) mają zostać zresetowane.

Zasięg dla wkładki

- W przypadku wkładek aplikacja AirKey pokaże wszystkie będące w zasięgu i aktywne wkładki Bluetooth, gdy zostaną one aktywowane poprzez ręczny dotknięcie.
- Wybrać określoną wkładkę i oddalić się od niej na wybraną odległość, tak aby zadziałało automatyczne rozpoznawanie smartfona.
- Nacisnąć ***Zapisz.***

Zasięg dla czytnika naściennego

- W przypadku czytników naściennych aplikacja AirKey pokaże wszystkie będące w zasięgu i aktywne czytniki naścienne Bluetooth.
- Wybrać określony czytnik naścienny i oddalić się od niego na wybraną odległość, tak aby zadziałało automatyczne rozpoznawanie smartfona.
- Nacisnąć ***Zapisz.***

Jednocześnie siła sygnału będzie wskazywana na wyświetlaczu. Proszę pamiętać, że ta wartość jest zależna od wpływów otoczenia, takich jak obciążenie falami radiowymi itp. i może być różna w zależności od smartfona.

Standardowy zasięg wynosi ok. 50-70 cm, ale jest ona zależna od producenta i urządzenia. Ze względów bezpieczeństwa firma EVVA zaleca, aby ustawić zasięg na ok. 30 cm.

Resetowanie wszystkich zasięgów Bluetooth

Naciskając przycisk ***Resetuj wszystkie zasięgi Bluetooth***, można usunąć wszystkie ręcznie ustawione zasięgi i przywrócić standardowe wielkości zasięgów. Komunikat informacyjny potwierdzi zresetowanie zasięgów.

6.9.4 Tryb "Hands free"

Umieść zaznaczenie w polu ***Tryb "Hands free"***, aby aktywować tę funkcję. Bliższe informacje na ten temat można znaleźć w rozdziale Przegląd trybu "Hands-free".

6.9.5 Odblokowanie z powiadomień

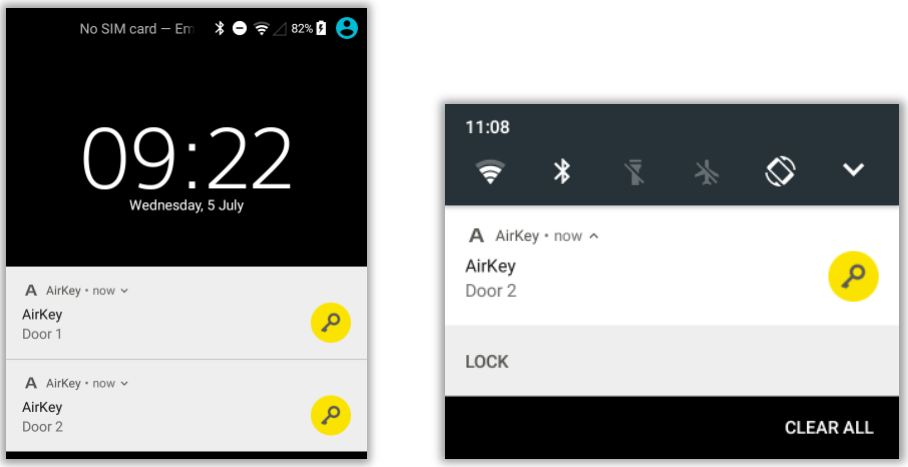
W przypadku tej funkcji możliwe jest odryglowanie komponentów zamykających AirKey poprzez Bluetooth, bez otwierania aplikacji AirKey.

Umieść zaznaczenie w polu ***Odblokowanie z powiadomień***, aby aktywować tę funkcję.

W przypadku smartfonów z systemem Android aktywowanie tej funkcji uruchomi usługę. Ta usługa nieustannie wyszukuje komponentów zamykających Bluetooth pozostających w zasięgu również po zamknięciu aplikacji AirKey, co prowadzi do zwiększonego zużycia akumulatora w smartfonie. Usługa zostanie wyłączona po dezaktywacji funkcji. Po naciśnięciu powiadomienia o usłudze nastąpi bezpośrednie przejście do ustawień aplikacji AirKey.

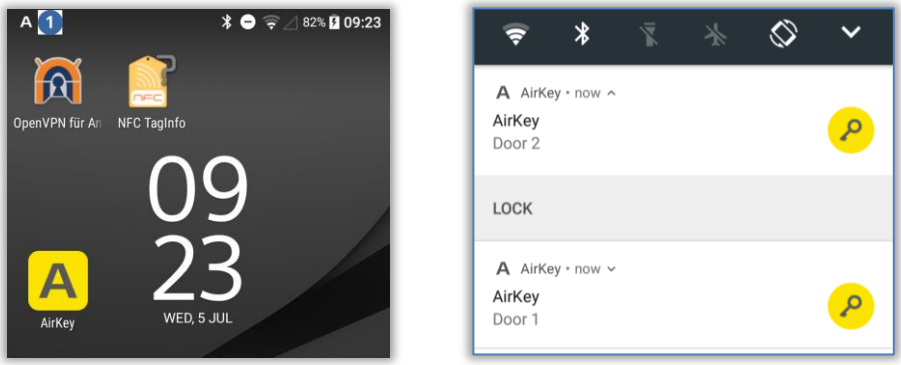
Gdy smartfon znajdzie się w zasięgu komponentu zamykającego AirKey, dla którego użytkownik posiada uprawnienie dostępu, pojawi się powiadomienie na zablokowanym

ekranie lub ekranie głównym smartfona. Za pomocą tego powiadomienia można wówczas zablokować komponent zamykający.



Rys. 217: Odblokowanie z powiadomień – ekran blokady

Powiadomienie na ekranie startowym smartfona ma postać litery **A** ❶, która pojawia się w lewym, górnym rogu. Po przesunięciu górnej krawędzi ekranu w dół zostaną wyświetlone powiadomienia informujące o tym, które komponenty zamykające można odryglować.



Rys. 218: Odblokowanie z powiadomień

W zależności do modelu smartfona interakcja z powiadomieniem będzie wymagać jednokrotnego dotknięcia powiadomienia lub rozłożenia smartfona, przesunięcia palcem lub naciśnięcia i przytrzymania powiadomienia, a następnie naciśnięcia przycisku ***Odblokuj***.

W zależności do ustawienia opcji ***Dostęp z ekranu blokady*** w ustawieniach Modułu zarządzania online systemu AirKey można albo odryglować bezpośrednio z ekranu blokady, albo konieczne będzie wcześniejsze usunięcie ekranu blokady. Szczegółowe informacje na ten temat można znaleźć w rozdziale Informacje ogólne.

Odblokowanie z powiadomień jest możliwe tylko wówczas, gdy powiadomienia dla komponentów w zasięgu zostały aktywowane w ustawieniach aplikacji AirKey. Konfigurację powiadomień opisano w rozdziale Powiadomienia.

6.9.6 Funkcje bezpieczeństwa

W menu ***Funkcje bezpieczeństwa*** znajdują się trzy poziomy bezpieczeństwa:

Szyfrowanie AirKey ❶
Funkcja działa jako dodatkowy kod PIN. Kod PIN składa się z 4–12 cyfr i chroni przed niepowołanym użyciem w razie zgubienia lub kradzieży smartfona.

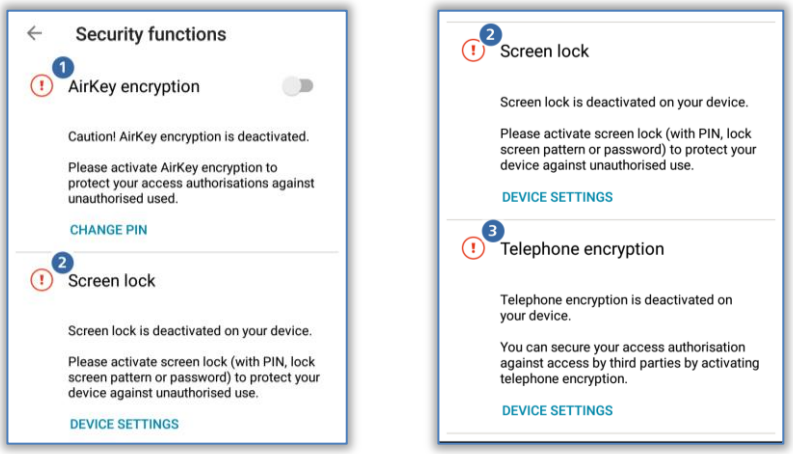
Firma EVVA zaleca stosowanie kodu PIN. Należy stosować możliwie długi kod PIN i zadbać o to, aby znał go tylko dany użytkownik!

Blokada ekranu ❷
Funkcja bezpieczeństwa systemu operacyjnego, która chroni ekran przed odblokowaniem przez osoby trzecie. Po wybraniu tej funkcji nastąpi bezpośrednie przekierowanie do ustawień smartfona Android.

Firma EVVA zaleca aktywowanie blokady ekranu. Jednocześnie należy zadbać o to, aby znał ją tylko właściciel smartfona.

Szyfrowanie telefonu ❸
Funkcja bezpieczeństwa systemu operacyjnego, która chroni smartfon przed odczytaniem danych przez osoby trzecie. Po wybraniu tej funkcji nastąpi bezpośrednie przekierowanie do ustawień systemu Android na smartfonie.

Firma EVVA zaleca aktywowanie funkcji szyfrowania telefonu. Należy przy tym uwzględnić wskazówki zawarte w instrukcji obsługi smartfona!

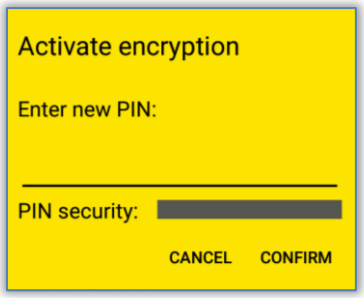


Rys. 219: Aplikacja AirKey – funkcje bezpieczeństwa

6.9.6.1 Aktywacja kodu PIN

Aby aktywować PIN, należy wykonać poniższe czynności:

- Otworzyć menu w aplikacji AirKey i stuknąć opcję ***Ustawienia*** → ***Funkcje bezpieczeństwa***.
- Aktywować opcję "Szyfrowanie AirKey".
- Wprowadzić kod PIN i stuknąć przycisk ***Potwierdź***.



Rys. 220: Aplikacja AirKey – aktywowanie kodu PIN

> Zakończyć procedurę, ponownie wprowadzając kod PIN i naciskając przycisk ***Potwierdź*** ab.

Firma EVVA zaleca stosowanie kodu PIN. Należy stosować możliwie długi kod PIN i zadbać o to, aby znał go tylko wybrany użytkownik. Już podczas wprowadzania kodu PIN siła hasła będzie wskazywana przez kolorowy pasek (czerwony / pomarańczowy / zielony).

Weryfikacja kodu PIN nastąpi dopiero podczas operacji blokowania komponentów zamykających. W ramach aplikacji nie nastąpi potwierdzenie prawidłowości kodu PIN. Kod PIN można także wcześniej skonfigurować i zapisać (patrz rozdział Wprowadzanie kodu PIN).

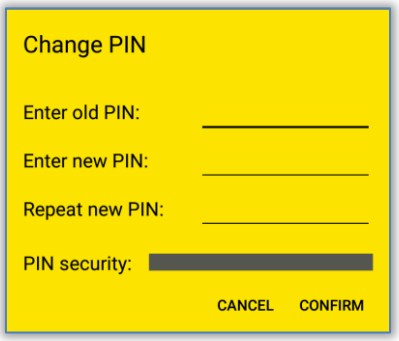
6.9.6.2 Zmiana kodu PIN

Aby zmienić skonfigurowany kod PIN w późniejszym czasie, należy wykonać następujące czynności:

> Otworzyć menu w aplikacji AirKey i stuknąć opcję ***Ustawienia*** → ***Funkcje bezpieczeństwa***.

> Kliknąć opcję ***Zmień PIN.***

> Wprowadzić stary kod PIN, wybrać nowy kod PIN, wprowadzić go ponownie i nacisnąć przycisk ***Potwierdź.***



Rys. 221: Aplikacja AirKey – zmiana kodu PIN

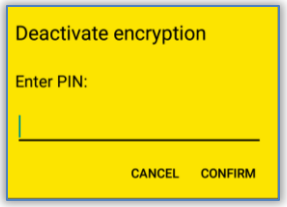
Należy stosować możliwie długi kod PIN i zadbać o to, aby znał go tylko wybrany użytkownik. Już podczas wprowadzania kodu PIN siła hasła będzie wskazywana przez kolorowy pasek (czerwony / pomarańczowy / zielony).

6.9.6.3 Dezaktywacja kodu PIN

Istnieją dwie możliwości dezaktywacji kodu PIN. Jeśli użytkownik zna kod PIN, można go dezaktywować bezpośrednio poprzez funkcje bezpieczeństwa smartfona. Jeśli kod PIN nie jest znany użytkownikowi, można go zresetować poprzez Moduł zarządzania online systemu AirKey, przy pomocy administratora.

Jeśli kod PIN jest znany, należy wykonać poniższą procedurę:

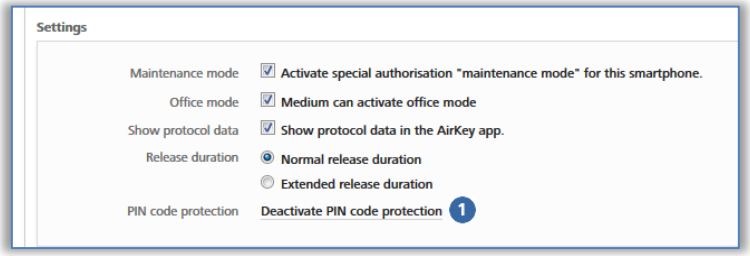
- Otworzyć menu w aplikacji AirKey i stuknąć opcję ***Ustawienia*** → ***Funkcje bezpieczeństwa***.
- Dezaktywować opcję "Szyfrowanie AirKey".
- Wprowadzić aktualny kod PIN i nacisnąć przycisk ***Potwierdź.***



Rys. 222: Aplikacja AirKey – dezaktywacja szyfrowania

Jeśli użytkownik nie zna kodu PIN, kod można zmienić w następujący sposób za pomocą Modułu zarządzania online systemu AirKey:

- Zalogować się jako administrator w systemie zamknięć.
- Na stronie startowej ***Home*** kliknąć ikonę ***Smartfony***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć smartfon, dla którego nastąpi dezaktywacja kodu PIN.
- Wybrać zakładkę ***Szczegóły*** w celu edycji informacji szczegółowych.
- Kliknąć opcję ***Dezaktywacja kodu PIN*** ❶ w bloku "Ustawienia".



Rys. 223: Moduł zarządzania online systemu AirKey – dezaktywowanie kodu PIN

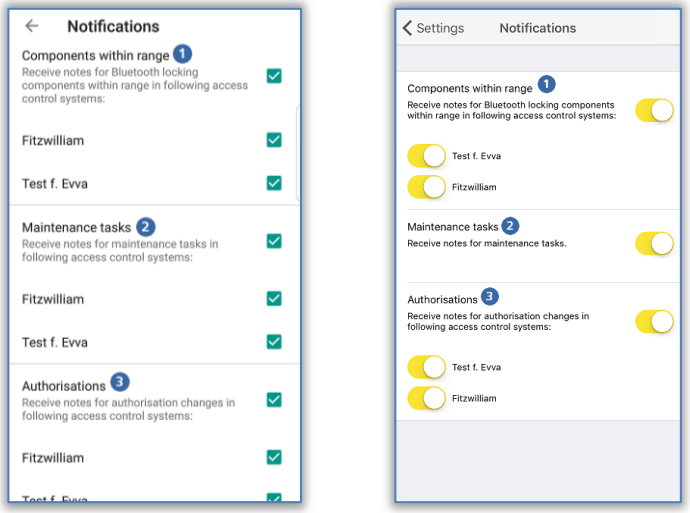
- Potwierdzić pytanie bezpieczeństwa przyciskiem ***Dezaktywuj kod PIN***.

Rys. 224: Moduł zarządzania online systemu AirKey – dezaktywowanie kodu PIN

Kod PIN można w dowolnym momencie ponownie aktywować.

6.9.7 Powiadomienia

W punkcie menu ***Ustawienia*** → ***Powiadomienia*** użytkownik może aktywować wysyłanie wiadomości typu push (informacje na ekranie blokady lub ekranie startowym smartfona) do komponentów w zasięgu, zadań konserwacyjnych i uprawnień lub ich zmian. Jeśli smartfon jest zarejestrowany w kilku systemach AirKey i dysponuje uprawnieniem konserwacyjnym, wówczas te systemy zamknięć także będą wyświetlone i można je wybrać.



Rys. 225: Aplikacja AirKey – ustawienia wiadomości push w smartfonie Android / iPhone

Powiadomienia dla *komponentów w zasięgu* 1

Jeśli to ustawienie jest aktywowane, użytkownik będzie otrzymywać odpowiednie wiadomości typu push na ekranie blokady lub ekranie startowym swojego smartfona, gdy smartfon znajdzie się w zasięgu komponentu zamykającego z funkcją Bluetooth. Z poziomu tych wiadomości można odryglować określone drzwi bez konieczności ręcznego otwierania aplikacji AirKey (szczegóły w rozdziale Odblokowanie z powiadomień).

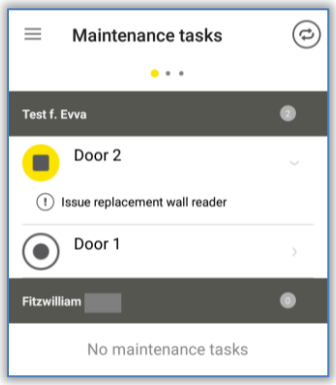
To ustawienie jest wyświetlane tylko przez smartfony z obsługą Bluetooth 4.0 (Bluetooth Low Energy).

Powiadomienia dla *zadań konserwacyjnych* 2

To ustawienie jest wyświetlane tylko na smartfonie z uprawnieniem konserwacyjnym.

Jeśli ustawienie jest aktywne, w menu głównym aplikacji AirKey pojawi się dodatkowo punkt menu ***Zadania konserwacyjne***. Na odpowiedniej stronie zostaną wyszczególnione komponenty zamykające i ich zadania konserwacyjne, utworzone w Module zarządzania online systemu AirKey.

Jeśli smartfon jest zarejestrowany w kilku systemach zamknięć, będą wyświetlone tylko te komponenty zamykające systemów zamknięć, dla których smartfon posiada uprawnienie do konserwacji. Gdy powstanie nowe zadanie konserwacyjne w Module zarządzania online systemu AirKey, użytkownik otrzyma na swoim smartfonie odpowiednie powiadomienie typu push.

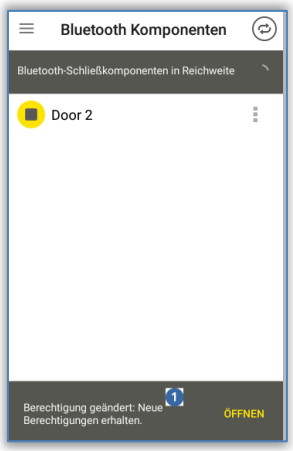


Rys. 226: Zadania konserwacyjne

Powiadomienia dla *uprawnień* ❸

To ustawienie jest zawsze wyświetlane.

Gdy to ustawienie jest aktywowane i zostanie zmienione lub utworzone nowe uprawnienie dla danego smartfona w Module zarządzania online systemu AirKey, użytkownik otrzyma informację ❶ wyświetloną przez ok. 2 s przy dolnej krawędzi ekranu aplikacji AirKey, jeśli jest ona otwarta.



Rys. 227: Powiadomienie o zmianie uprawnienia

Jeśli aplikacja AirKey nie jest otwarta, użytkownik otrzyma odpowiednie powiadomienie typu push na ekranie blokady lub ekranie startowym swojego smartfona.

Niezależnie od ustawienia dla powiadomień o uprawnieniach użytkownik otrzyma długotrwały wpis na stronie protokół uprawnień.

6.9.8 Dodawanie systemu zamknięć

Smartfony mogą być zarejestrowane w więcej niż jednym systemie zamknięć AirKey. Jeśli określony smartfon ma być dodany do kolejnego systemu zamknięć, wówczas można za pomocą funkcji ***Dodaj system zamknięć*** wprowadzić kod rejestracji. Bliższe informacje na ten temat można znaleźć w rozdziale Używanie smartfona w kilku systemach.

6.9.9 Informacje

Aplikacja AirKey dysponuje funkcją umożliwiającą wyświetlenie aktualnie zainstalowanej wersji aplikacji, szczegółów rejestracji smartfona, identyfikatorów nośników smartfona oraz ogólnych warunków licencyjnych firmy EVVA.

> Uruchomić aplikację AirKey.

> W menu nacisnąć opcję ***Ustawienia*** → ***Informacja***.

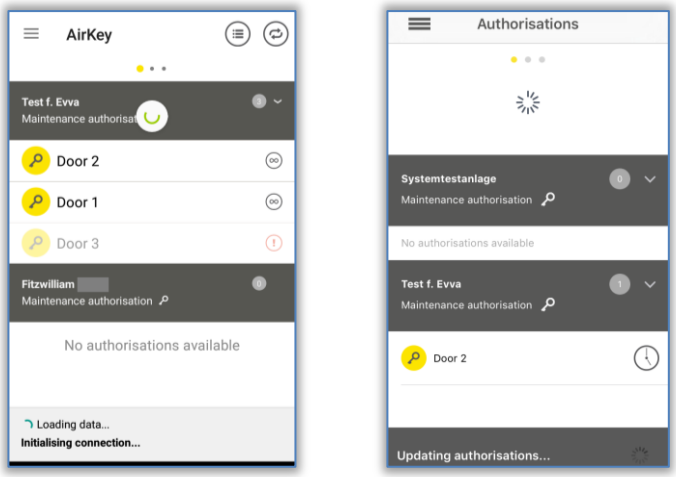
Rys. 228: Aplikacja AirKey – informacje

6.10 Aktualizacja smartfona

Aby smartfon dysponował aktualnymi danymi systemu zamknięć AirKey, w dowolnym momencie można wykonać ręczną aktualizację smartfona za pośrednictwem modułu zarządzania online.

W tym celu w przypadku smartfona Android należy na stronie "Uprawnienia" aplikacji AirKey przesunąć palcem z góry na dół ekranu. Pojawi się symbol aktualizacji (obracające się kółko).

W przypadku iPhone'a należy przesunąć stronę "Uprawnienia" do dolnej krawędzi. Pojawi się symbol aktualizacji (obracające się promienie).



Rys. 229: Aktualizacja smartfona Android lub iPhone'a

W przypadku zmian dotyczących smartfona system AirKey korzysta z wiadomości typu push (powiadomienia). W ten sposób następuje automatyczna aktualizacja smartfona. Nie można zagwarantować dostarczenia wiadomości typu push. Dlatego należy skontrolować, czy wiadomości zostały dostarczone i ewentualnie wykonać aktualizację ręcznie.

Smartfon jest aktualizowany automatycznie po uruchomieniu aplikacji AirKey albo smartfon co 12 godzin automatycznie próbuje wykonać aktualizację, jeżeli aplikacja AirKey jest w tym czasie uruchomiona.

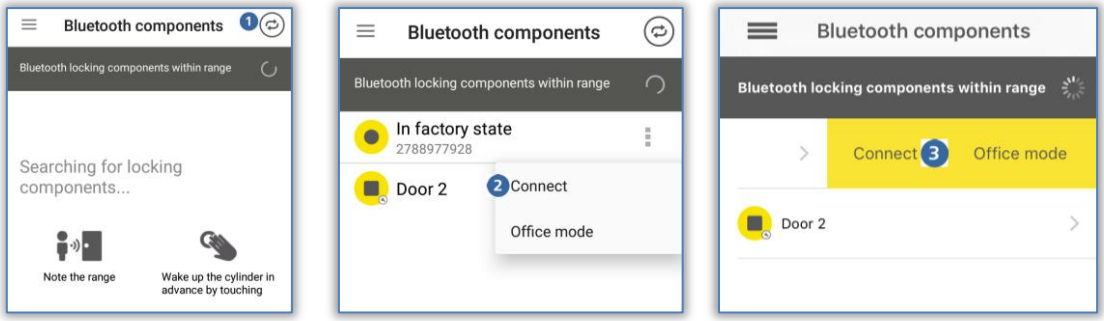
W dolnej sekcji aplikacji AirKey w momencie aktualizacji wyświetli się informacja o stanie aktualizacji. Gdy ta informacja przestanie być wyświetlana, oznacza to, że aktualizacja została ukończona.

Opcjonalnie aktualizacja może następować po każdym dostępie. Jednak w tym celu funkcja "Aktualizacja po każdym dostępie" musi być uaktywniana w odnośnym systemie zamknięć AirKey. Uaktywnianie i szczegóły tej funkcji są opisane w rozdziale Informacje ogólne.

6.11 Połączenie z komponentem

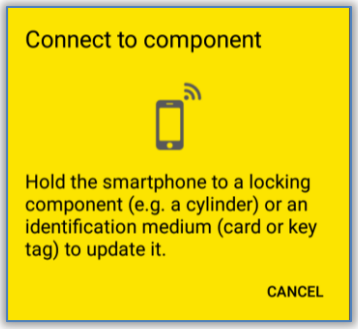
Za pomocą smartfona można zaktualizować każdy nośnik dostępu (z wyjątkiem smartfonów) i każdy komponent zamykający AirKey, niezależnie od przynależności do jego systemu zamknięć.

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.
- Utworzenie połączenia **Bluetooth** (w smartfonach Android): W menu kontekstowym stuknąć komponent zamykający, z którym ma zostać nawiązane połączenie (⋮), a następnie wybrać opcję ***Połącz*** ❷.
- Utworzenie połączenia **Bluetooth** (w iPhone'ach): Przy komponencie zamykającym, z którym ma zostać nawiązane połączenie, przesunąć nazwę komponentu w lewo i wybrać opcję ***Połącz*** ❸.



Rys. 230: Aplikacja AirKey – połączenie z komponentem: Android NFC / Android Bluetooth / iPhone

> Postępować zgodnie z instrukcjami i przytrzymać smartfon z obsługą NFC przy nośniku lub komponencie zamykającym, lub smartfon z obsługą Bluetooth w zasięgu komponentu zamykającego.



Rys. 231: Aktualizacja danych

Następuje aktualizacja danych. Podczas przesyłania nie wolno odsuwać smartfona od aktualizowanego komponentu. Gdy operacja zostanie zakończona, pojawi się odpowiedni komunikat.

Dezaktywuj tryb "Hands free" przed połączeniem z komponentem zamykającym Bluetooth. W przeciwnym razie może dojść do przerwania połączenia.

Komponenty zamykające Bluetooth można również automatycznie aktualizować po każdej operacji odryglowania poprzez Bluetooth. Bliższe informacje na temat funkcji "Aktualizacja po każdym odblokowaniu" znajdują się w części Wartości domyślne (dla wszystkich nowo dodanych komponentów zamykających).

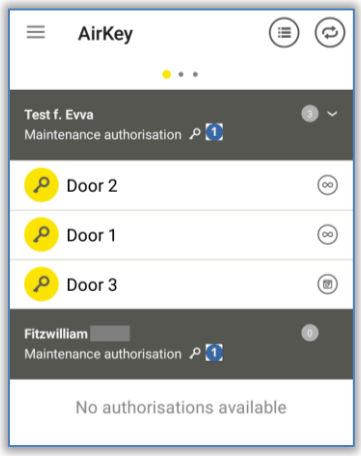
Komponenty AirKey należy regularnie aktualizować. Tylko w ten sposób można zapewnić bezpieczeństwo i aktualność danych w systemie AirKey. Dalsze informacje na temat aktualizacji komponentów AirKey można znaleźć w rozdziale Eksploatacja i konserwacja systemu AirKey.

6.12 Specjalne uprawnienie "uprawnienie do konserwacji"

Jeśli dla określonego smartfona aktywowano w Module zarządzania online systemu AirKey specjalne uprawnienie "uprawnienie do konserwacji", możliwe jest wykonanie dodatkowych czynności konserwacyjnych na komponentach AirKey. Uprawnienie do konserwacji uprawnia

użytkownika do odblokowania komponentów zamykających AirKey w stanie fabrycznym, dodawania i usuwania komponentów i nośników dostępu (z wyjątkiem smartfonów) w swoim systemie zamknięć AirKey, a także do aktualizowania firmware komponentów lub oprogramowania Keyring nośników, takich jak karta, brelok do kluczy i klucz Combi.

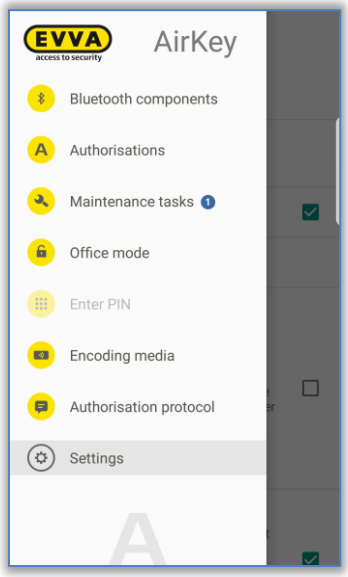
Uprawnienie do konserwacji można rozpoznać w aplikacji AirKey na stronie ***Uprawnienia*** jako pozycję "Uprawnienie do konserwacji" ❶ na szarym pasku.



Rys. 232: Uprawnienie do konserwacji

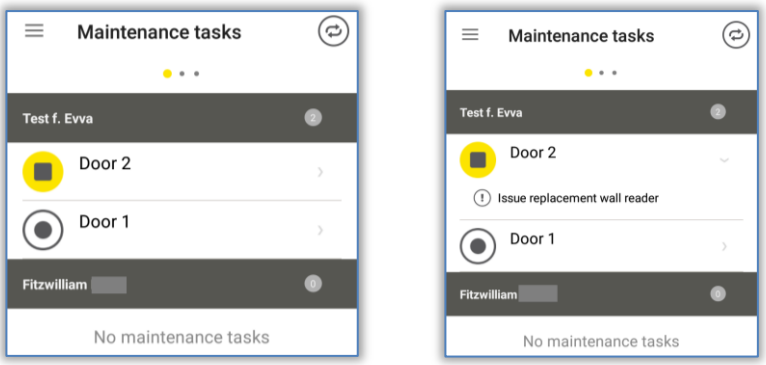
Uprawnienie do konserwacji można aktywować w polu "Szczegóły" odpowiedniego smartfona w Module zarządzania online systemu AirKey. Szczegółowe informacje na temat edycji nośnika znajdują się w rozdziale Edycja nośnika.

Dodatkowo, w menu głównym aplikacji AirKey zostanie udostępniony punkt ***Zadania konserwacyjne*** ❶.



Rys. 233: Punkt "Zadania konserwacyjne" w menu głównym

> Stuknąć tę opcję, aby wyświetlić listę zadań konserwacyjnych dla komponentów zamykających danego systemu. Po stuknięciu nazwy komponentu zamykającego zostanie wyświetlona lista otwartych zadań konserwacyjnych dla tego komponentu.



Rys. 234: Zadania konserwacyjne

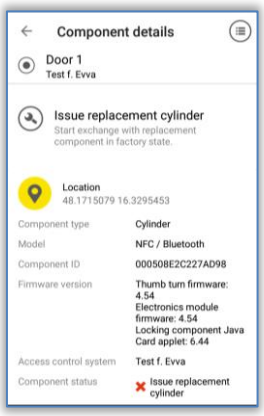
Technik zajmujący się konserwacją powinien regularnie sprawdzać listę zadań konserwacyjnych, aby niezwłocznie wykonywać aktualizację wyznaczonych komponentów zamykających.

Jeśli smartfon z uprawnieniem do konserwacji dostanie się w zasięg komponentu zamykającego z funkcją Bluetooth (wkładka ◉ lub czytnik naścienny ▣), symbol tego komponentu zostanie podświetlony na żółto (np. ● w przypadku wkładki).

Po stuknięciu żółtego symbolu zostanie nawiązane połączenie z komponentem zamykającym i nastąpi aktualizacja. Następnie zostaną wyświetlone szczegóły komponentu. Zaległa aktualizacja firmware będzie wskazana w szczegółach komponentu i z tego miejsca można ją uruchomić.

Dodatkowo użytkownik, pełniący funkcję technika konserwacyjnego, podczas aktualizacji komponentów zamykających może wyświetlić przegląd szczegółów komponentu. Dzięki temu można bezpośrednio sprawdzić status komponentu zamykającego i zdarzenia danej wkładki w ramach protokołu.

> Wykonać aktualizację komponentu zamykającego, aby wyświetlić szczegóły komponentu. Tutaj można także zobaczyć lokalizację komponentu zamykającego w formie współrzędnych GPS (o ile są dostępne) lub adres ręcznie wprowadzony w module zarządzania online. Po naciśnięciu żółtego symbolu lokalizacji nastąpi automatyczne przejście do operatora karty, który jest ustawiony jako standardowy na określonym smartfonie.



Rys. 235: Wyświetlenie szczegółów komponentu zamykającego

Komponenty AirKey należy regularnie aktualizować. Tylko w ten sposób można zapewnić bezpieczeństwo i aktualność danych w systemie AirKey. Dalsze informacje na temat aktualizacji komponentów AirKey można znaleźć w rozdziale Eksploatacja i konserwacja systemu AirKey.

Tryb konserwacji jest ważny tylko w tych systemach zamknięć, w których został aktywowany. Jednak można go aktywować jednocześnie w kilku systemach.

Tryb "Hands free" musi być dezaktywowany na smartfonie, aby możliwe było wykonanie zadań konserwacyjnych lub aktualizacji komponentów zamykających.

6.13 Dodawanie komponentu AirKey

Aby dodać do systemu zamknięć AirKey komponent zamykający lub nośnik dostępu (z wyjątkiem smartfona) za pomocą smartfona, należy aktywować tryb konserwacji dla systemu zamknięć a komponent AirKey musi być w stanie fabrycznym.

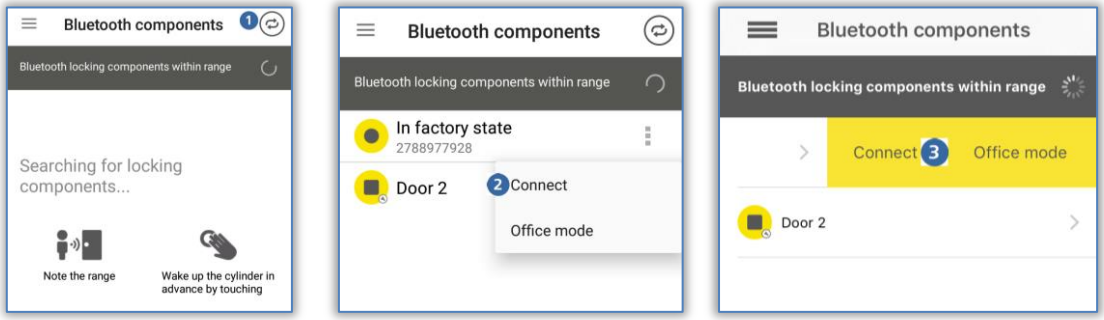
6.13.1 Dodawanie nośników: patrz rozdział 4.12

6.13.2 Dodawanie komponentu zamykającego: patrz rozdział 4.11

6.14 Usuwanie komponentu AirKey

Aby usunięcie było możliwe, komponent zamykający lub nośnik (z wyjątkiem smartfona) musi zostać najpierw usunięty w module zarządzania online (patrz rozdziały Usuwanie komponentu zamykającego i Usuwanie nośnika) a smartfon musi mieć aktywny tryb konserwacji.

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.
- Utworzenie połączenia **Bluetooth** (w smartfonach Android): W menu kontekstowym stuknąć komponent zamykający, z którym ma zostać nawiązane połączenie (⋮), a następnie wybrać opcję ***Połącz*** ❷.
- Utworzenie połączenia **Bluetooth** (w iPhone'ach**)**: Przy komponencie zamykającym, z którym ma zostać nawiązane połączenie, przesunąć nazwę komponentu w lewo i wybrać opcję ***Połącz*** ❸.

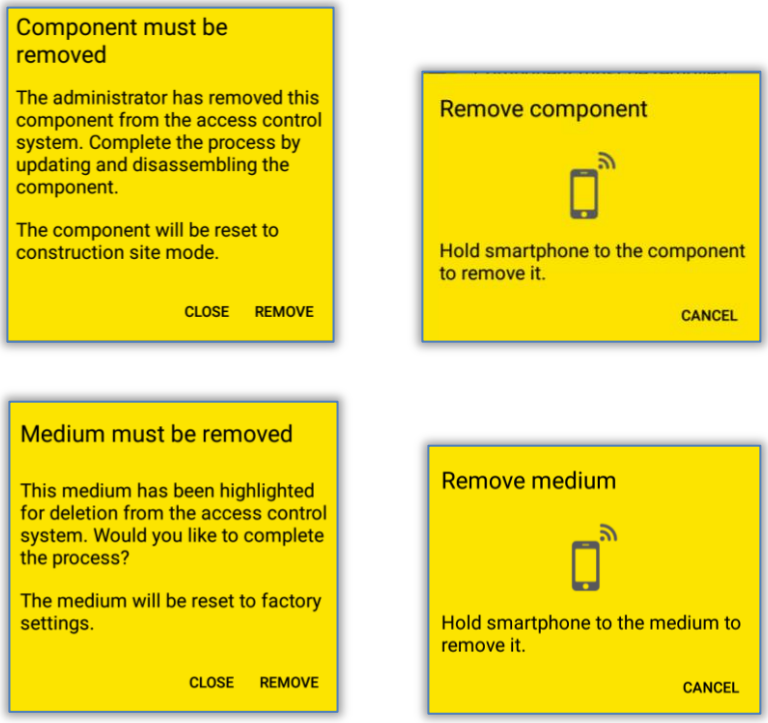


Rys. 236: Aplikacja AirKey – połączenie z komponentem: Android NFC / Android Bluetooth / iPhone

> Postępować zgodnie z instrukcjami i przytrzymać smartfon z obsługą NFC przy nośniku lub komponencie zamykającym, lub smartfon z obsługą Bluetooth w zasięgu komponentu zamykającego.

Rys. 237: Aplikacja AirKey – połączenie z komponentem

Przytrzymać smartfon z obsługą NFC przy nośniku / komponencie AirKey, który został już usunięty w Module zarządzania online systemu AirKey lub przytrzymać smartfon Bluetooth w zasięgu usuwanego komponentu lub bezpośrednio przy usuwanym nośniku, a następnie postępować zgodnie z instrukcjami.

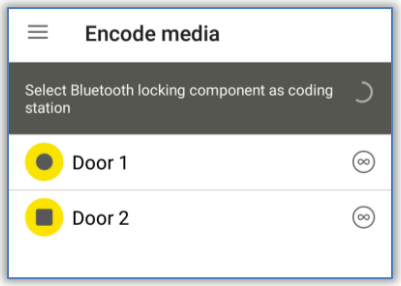


Rys. 238: Usuwanie komponentu AirKey

Po pomyślnym wykonaniu aktualizacji komponenty zamykające i nośniki są ponownie w stanie fabrycznym.

Jeśli nośnik dostępu ma zostać usunięty z systemu AirKey za pomocą iPhone'a, należy postępować analogicznie do procedury dodawania poprzez funkcję ***Koduj nośniki***.

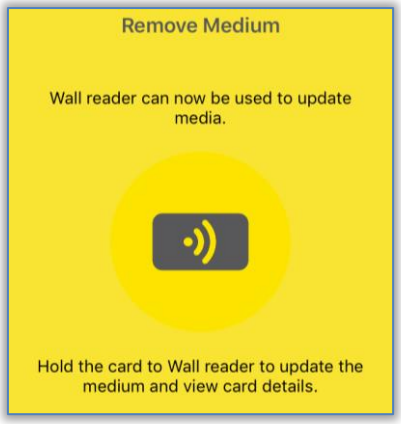
> Z listy wyświetlonych komponentów zamykających Bluetooth wybrać te, poprzez które ma nastąpić aktualizacja nośnika.



Rys. 239: Kodowanie nośników – lista wyboru komponentów Bluetooth

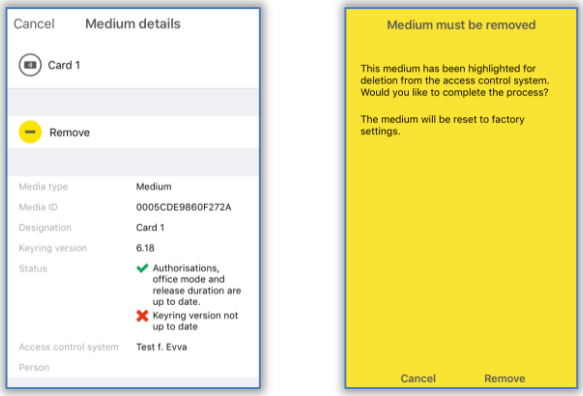
> Przytrzymać nośnik przeznaczony do aktualizacji przy komponencie zamykającym AirKey.

> Pojawi się wiadomość, że komponent zamykający AirKey jest gotowy.



Rys. 240: Usuwanie nośnika za pomocą iPhone'a

> Przytrzymać nośnik dostępu przy komponencie zamykającym AirKey i stuknąć opcję ***Usuń***.



Rys. 241: Usuwanie nośnika

> Pojawi się komunikat o pomyślnym usunięciu nośnika dostępu z systemu AirKey.

W żadnym wypadku nie wolno odsuwać smartfona od komponentu zamykającego lub nośnika podczas tej operacji.

Procedura usuwania komponentów zamykających i nośników (z wyjątkiem smartfona) jest identyczna.

Komponentów NFC nie można usunąć z systemu zamknięć za pomocą iPhone'a. Do tego celu potrzebna jest opcjonalna stacja kodująca lub smartfon Android z obsługą technologii NFC.

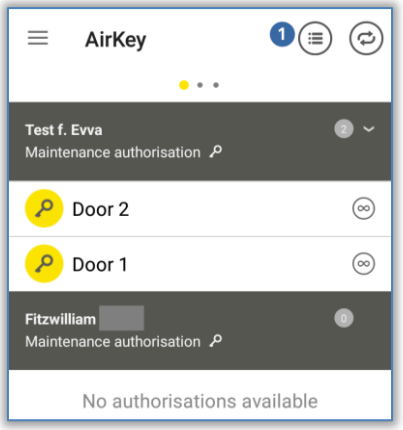
6.15 Dane z protokołów w aplikacji AirKey

W przypadku smartfonów uprawnienie do wyświetlenia danych z protokołów można udostępnić przez Moduł zarządzania online systemu AirKey. Wyświetlanie danych protokołowych jest niezależne od uprawnienia do konserwacji i może być uaktywnione przez każdego.

Wyświetlanie danych z protokołów można aktywować lub dezaktywować w Module zarządzania online systemu AirKey w polu "Szczegóły" określonego smartfona. Szczegółowe informacje na temat edycji nośnika znajdują się w rozdziale Edycja nośnika.

Protokoły można wywołać w aplikacji w następujący sposób:

- Uruchomić aplikację AirKey.
- W menu głównym wybrać opcję ***Uprawnienia***.
- Wybrać symbol protokołu ❶, znajdujący się w górnym prawym rogu ekranu.



Rys. 242: Symbol protokołu

- Zostanie wyświetlony protokół.

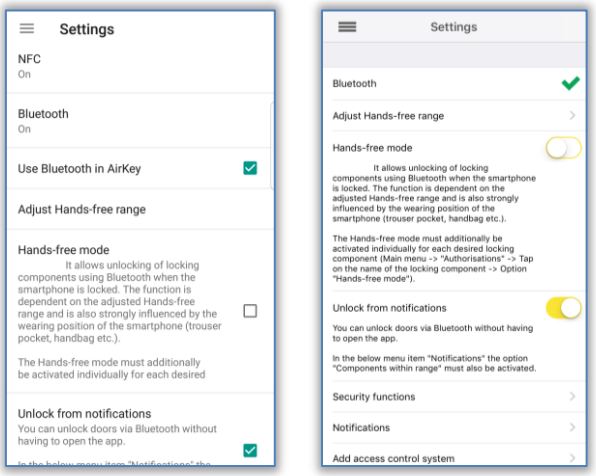
W ramach protokołu aplikacji AirKey będą wyświetlone wyłącznie wpisy do protokołu tej osoby, do której przypisano smartfon.

6.16 Przegląd trybu "Hands-free"

Komponenty zamykające Bluetooth mają możliwość użytkowania w trybie Hands-free. Jednocześnie chodzi tu o funkcję zwiększającą komfort, w przypadku której nie będzie już konieczne wybieranie komponentu zamykającego w aplikacji. Funkcji "Hands-free" nie należy utożsamiać z funkcją odryglowania poprzez Bluetooth, natomiast można ją aktywować dla większego komfortu obsługi.

Po dotknięciu, wkładka wysyła sygnał Bluetooth. W przypadku czytnika naściennego odbywa się to automatycznie, bez dotknięcia. Jeśli aplikacja mobilna AirKey w zasięgu odryglowania odbierze ten sygnał Bluetooth, zostanie rozpoczęty proces odryglowania. Zasięg odryglowania można indywidualnie ustawić w aplikacji dla wkładki i czytnika naściennego.

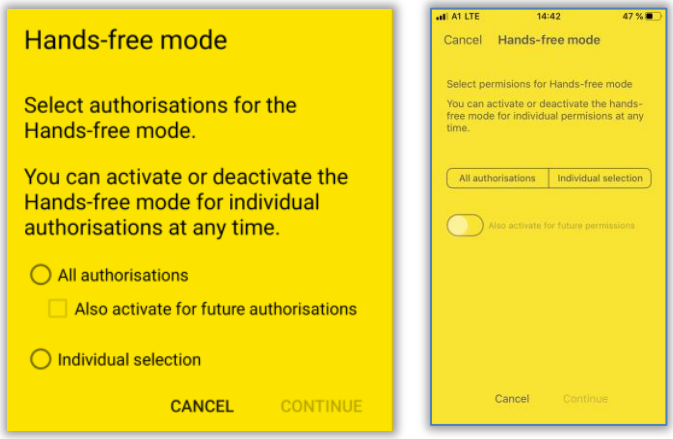
> W aplikacji AirKey, w menu głównym w oknie ***Ustawienia*** należy aktywować tryb Hands-free.



Rys. 243: Ustawienia aplikacji AirKey

W przypadku smartfonów z systemem Android aktywowanie tej funkcji uruchomi usługę. Ta usługa nieustannie wyszukuje komponenty zamykające Bluetooth pozostające w zasięgu również po zamknięciu aplikacji AirKey, co prowadzi do zwiększonego zużycia akumulatora w smartfonie. Usługa zostanie wyłączona po dezaktywacji funkcji. Po naciśnięciu powiadomienia o usłudze nastąpi bezpośrednie przejście do ustawień aplikacji AirKey.

> Dodatkowo dla każdego komponentu zamykającego lub strefy w szczegółach uprawnienia w punkcie menu ***Uprawnienia*** należy aktywować tryb Hands free. Podczas pierwszej aktywacji trybu "Hands free" pojawi się okno dialogowe, w którym funkcję można automatycznie aktywować dla wszystkich komponentów zamykających lub indywidualnie tylko dla poszczególnych komponentów zamykających.



Rys. 244: Uprawnienia trybu Hands free

Aktywuj opcję ***Aktywuj również dla przyszłych uprawnień***, aby automatycznie aktywować tryb "Hands free" również dla każdego kolejnego uprawnienia.

W zależności do ustawienia opcji ***Dostęp z ekranu blokady*** w ustawieniach Modułu zarządzania online systemu AirKey można albo odryglować bezpośrednio z ekranu blokady, albo konieczne będzie wcześniejsze usunięcie ekranu blokady. Szczegółowe informacje na ten temat można znaleźć w rozdziale Informacje ogólne.

Ustawianie zasięgu trybu Hands-free: patrz rozdział 6.9.3

O czym należy pamiętać podczas korzystania z trybu "Hands free"?

Działanie podczas zablokowanego ekranu smartfona jest zależne

- od ustawienia "Dostęp z ekranu blokady" w ustawieniach modułu zarządzania online;
- od producenta, systemu operacyjnego, wieku, liczby zainstalowanych aplikacji, optymalizacji aplikacji (funkcja oszczędzania energii) smartfona;
- od czynników zakłócających, takich jak rodzaj budynku (np. obiekt z żelbetu) oraz otoczenie radiowe;
- od miejsca przechowywania lub noszenia smartfona oraz od ustawionego zasięgu odryglowania dla funkcji "Hands-free";
- od tego, czy smartfon łączy się właśnie z siecią WLAN.

Ze względu na te czynniki funkcja "Hands-free" może działać wolniej lub ewentualnie może w ogólne nie działać. Aby przyspieszyć proces odryglowania w trybie "Hands-free", w zależności od systemu operacyjnego (np. iOS) należy smartfon odblokować oraz uruchomić aplikację AirKey. W takim przypadku można pominąć wybór odblokowywanych komponentów w aplikacji.

Aby uniknąć niezamierzonego odryglowania, należy uwzględnić następujące czynniki:

- Po każdej operacji odryglowania następuje w przypadku czytników naściennych tzw. "time-out" trwający 2 minuty. To oznacza, że czytnik naścienny można ponownie odryglować w trybie "Hands-free", gdy przez 2 minuty smartfon nie będzie znajdować się w zasięgu odryglowania czytnika naściennego. W ten sposób można uniknąć niezamierzonego odryglowania podczas opuszczania zasięgu odryglowania.
- W odpowiednim przypadku zawsze znajduje się tylko jeden komponent zamykający w zasięgu odryglowania smartfona.
- Aby wykonać funkcje takie jak np. "Koduj nośniki" lub "Aktualizuj komponenty zamykające", należy dezaktywować tryb "Hands free" w aplikacji.

7 Obsługa komponentów zamykających AirKey

7.1 Dostęp za pomocą smartfona

Aby uzyskać dostęp do komponentu zamykającego AirKey, muszą być spełnione następujące warunki:

- Na smartfonie włączono funkcję NFC lub Bluetooth.
- Aplikacja AirKey jest zainstalowana i zarejestrowana.
- Zostało przydzielone ważne uprawnienie do smartfona (szczegółowe informacje można znaleźć w rozdziałach Rejestracja smartfona i Przydzielanie uprawnień).
- Przytrzymać smartfon przy komponencie zamykającym podczas odryglowania poprzez NFC. Położenie zapewniające najlepsze możliwości odczytu zależą od modelu smartfona. Zasięg odczytu jest zależny od typu smartfona i z reguły wynosi od zera do kilku milimetrów. Podczas procesu odryglowania poprzez Bluetooth zasięg odczytu z jednej strony jest zależny od typu smartfona, a z drugiej strony od indywidualnych ustawień w aplikacji AirKey na smartfonie dla trybu Hands-free. Zasięg ten może wynosić do kilku metrów.
- Jeśli wymagane jest wprowadzenie kodu PIN, należy wprowadzić właściwy kod, zanim możliwe będzie wykonanie odryglowania za pomocą smartfona poprzez NFC lub Bluetooth. (Szczegóły dotyczące kodu PIN znajdują się w rozdziale Funkcje bezpieczeństwa).
- Zwracać uwagę na optyczną sygnalizację komponentu zamykającego. W razie połączenia NFC nie odsuwać smartfona od komponentu zamykającego lub w razie połączenia Bluetooth pozostać w zasięgu odbioru, aż komponent zamykający zasygnalizuje kolorem zielonym. (Sygnalizacja kolorem niebieskim oznacza tylko komunikację między smartfonem a komponentem zamykającym.)

Za pomocą modeli iPhone XR, XS, XS Max i nowszych można również odryglować komponenty Bluetooth poprzez połączenie NFC. W tym celu należy przytrzymać smartfon przy komponencie zamykającym i dotknąć komunikat informacyjny o rozpoznaniu etykiety NFC. Następnie zostanie otwarta aplikacja AirKey i będzie przeprowadzona operacja odryglowania poprzez Bluetooth.

Rys. 245: Etykieta iOS NFC

Sprawdzić uprawnienie lub kod PIN, jeśli sygnalizacja komponentu zamykającego ma kolor czerwony.

Blokowanie komponentów zamykających poprzez NFC nie jest możliwe w trakcie aktywnej blokady ekranu lub podczas połączenia telefonicznego. Jednak aplikacja AirKey nie musi być uruchomiona ani działać na pierwszym planie, aby możliwe było odryglowanie komponentów zamykających. Natomiast odryglowanie komponentów zamykających poprzez Bluetooth jest możliwe przy aktywnej blokadzie ekranu za pośrednictwem wiadomości typu push. Należy jednak w ustawieniach aplikacji AirKey aktywować opcję "Odblokowanie z powiadomień" oraz w ustawieniach modułu zarządzania online umożliwić "Dostęp z ekranu blokady".

7.2 Dostęp za pomocą nośników takich jak karty, breloki do kluczy, bransoletki lub klucze Combi

Aby uzyskać dostęp umożliwiony przez komponent zamykający AirKey, nośnik musi być dodany do systemu zamknięć i posiadać ważne uprawnienie (szczegółowe informacje na ten temat można znaleźć w rozdziałach Dodawanie kart, breloków do kluczy i kluczy Combi za pomocą smartfona i Przydzielanie uprawnień).

- Przytrzymać nośnik przy komponencie zamykającym. Zasięg odczytu jest zależny od typu nośnika i z reguły wynosi kilka milimetrów.
- Zwracać uwagę na optyczną sygnalizację komponentu zamykającego. Nie odsuwać nośnika, zanim komponent nie zasygnalizuje zielonym kolorem. (Sygnalizacja kolorem niebieskim oznacza tylko komunikację między nośnikiem a komponentem zamykającym.)

Sprawdzić uprawnienie, jeśli sygnalizacja komponentu zamykającego ma kolor czerwony.

- Komponent zamykający odblokuje się na określony okres zezwolenia i użytkownik uzyska żądany dostęp.

Nośniki, takie jak karty, breloki do kluczy, bransoletki lub klucze Combi, mogą działać w ograniczonym stopniu lub w ogóle nie działać w pobliżu innych nośników lub przedmiotów metalowych. Może to dotyczyć np. nośników w portmonetce lub w pęku kluczy.

Identyfikację za pomocą klucza Combi należy wykonywać przy komponentach zamykających z tej strony, na której znajduje się symbol RFID.

8 Eksploatacja i konserwacja systemu AirKey

8.1 Aktualizowanie komponentów zamykających

Użytkownik może zaktualizować zasadniczo każdy komponent zamykający AirKey, niezależnie od przynależności do systemu zamknięć, aby przeprowadzić wymianę danych pomiędzy Modułem zarządzania online systemu AirKey i komponentem zamykającym.

Aktualizację można przeprowadzić za pomocą smartfona lub stacji kodującej. Aktualizacja za pomocą smartfona wymaga jednak instalacji aplikacji AirKey i rejestracji w wybranym systemie zamknięć.

Podczas aktualizacji komponentów zamykających wykonywane są następujące operacje:

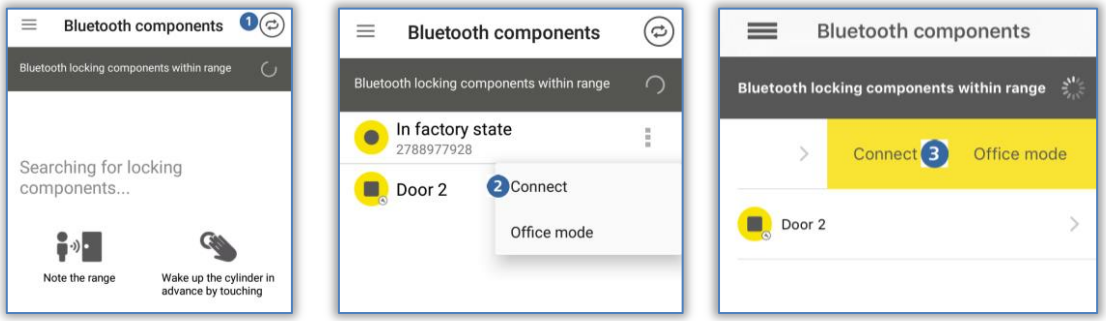
- Ustawiana jest na nowo godzina.
- Następuje odczyt wpisów do protokołu oraz stanu baterii.
- Następuje aktualizacja zadań konserwacyjnych (czarna lista, udostępnienia do innych systemów itd.).
- Zostają odczytane szczegóły komponentu.

Aby wykonać aktualizację komponentu zamykającego za pomocą smartfona, należy wykonać następujące czynności:

> Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.

> Utworzenie połączenia **Bluetooth** (w smartfonach Android): W menu kontekstowym stuknąć komponent zamykający, z którym ma zostać nawiązane połączenie (⋮), a następnie wybrać opcję ***Połącz*** ❷.

> Utworzenie połączenia **Bluetooth** (w iPhone'ach**)**: Przy komponencie zamykającym, z którym ma zostać nawiązane połączenie, przesunąć nazwę komponentu w lewo i wybrać opcję ***Połącz*** ❸.



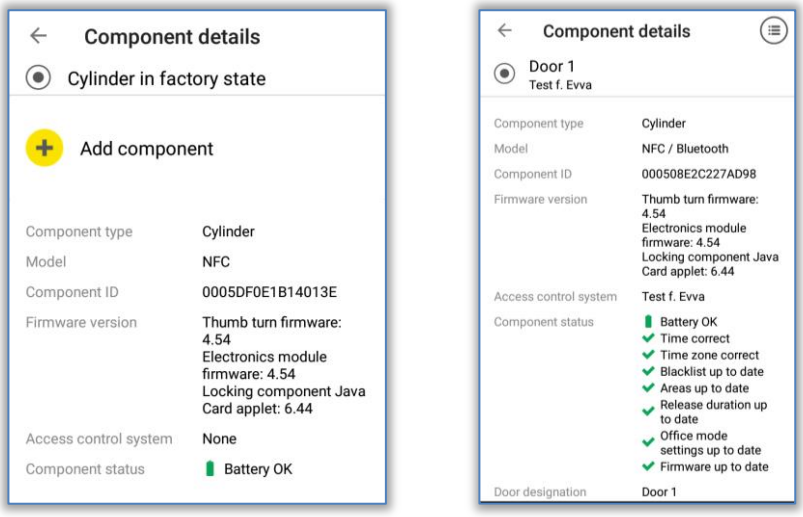
Rys. 246: Aplikacja AirKey – połączenie z komponentem: Android NFC / Android Bluetooth / iPhone

> Postępować zgodnie z instrukcjami.

Rys. 247: Aktualizacja danych

Następuje aktualizacja danych. Podczas transmisji nie wolno odsuwać smartfona z funkcją NFC od synchronizowanego komponentu lub ew. nie wolno usuwać smartfona z funkcją Bluetooth z zasięgu komponentu zamykającego. Gdy operacja zostanie zakończona, pojawi się odpowiedni komunikat.

W zależności od tego, czy na smartfonie aktywowano tryb konserwacji i czy komponent zamykający znajduje się we własnym lub obcym systemie zamknięć AirKey, wyświetlane informacje komunikatów aktualizacyjnych mogą się różnić.



Rys. 248: Komunikaty aktualizacyjne

Dezaktywuj tryb "Hands free" przed połączeniem z komponentem zamykającym Bluetooth. W przeciwnym razie może dojść do przerwania połączenia.

Komponenty zamykające Bluetooth można również automatycznie aktualizować po każdej operacji odryglowania poprzez Bluetooth. Bliższe informacje na temat funkcji "Aktualizacja po każdym odblokowaniu" znajdują się w części Wartości domyślne (dla wszystkich nowo dodanych komponentów zamykających).

Option

Aktualizowanie komponentu zamykającego za pomocą stacji kodującej

Aby zaktualizować komponent zamykający za pomocą stacji kodującej, należy wykonać poniższą procedurę:

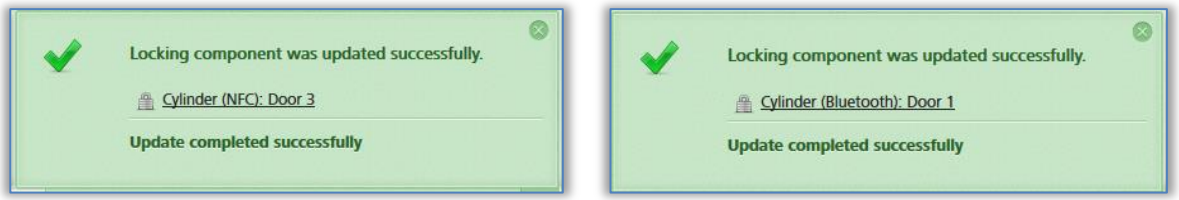
> Zalogować się do systemu zamknięć AirKey i sprawdzić, czy stacja kodująca została podłączona i wybrana w module zarządzania online.

> Położyć komponent zamykający na stację kodującą.

Rys. 249: Aktualizowanie komponentu zamykającego za pomocą stacji kodującej

> Usunąć komponent zamykający ze stacji kodującej dopiero wówczas, gdy aktualizacja zostanie pomyślnie zakończona i pojawi się odpowiedni komunikat.

W zależności od tego, czy komponent zamykający znajduje się we własnym lub obcym systemie zamknięć AirKey, wyświetlane informacje komunikatów o pomyślnej realizacji mogą się różnić.



Rys. 250: Aktualizowanie komponentu zamykającego za pomocą stacji kodującej

Komponenty zamykające AirKey należy regularnie aktualizować. Tylko w ten sposób można zapewnić bezpieczeństwo i aktualność danych w systemie AirKey.

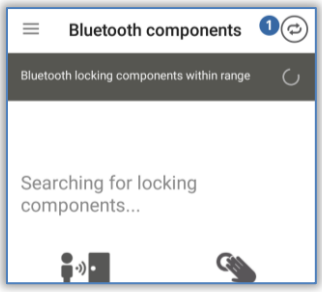
8.2 Aktualizacja smartfona: patrz rozdział 6.10

8.3 Aktualizowanie nośników

Użytkownik może zaktualizować każdy nośnik AirKey, niezależnie od przynależności do systemu zamknięć. Aktualizację można przeprowadzić za pomocą smartfona z systemem Android lub opcjonalnej stacji kodującej. Aktualizacja za pomocą smartfona wymaga jednak instalacji aplikacji AirKey i rejestracji w wybranym systemie zamknięć.

W przypadku iPhone'a nośniki są aktualizowane analogicznie do funkcji Koduj nośniki, stosując komponent zamykający AirKey jako stację kodującą.

> W przypadku smartfona z systemem Android stuknąć symbol ***Połącz z komponentem*** ❶ z prawej strony, u góry ekranu aplikacji AirKey.



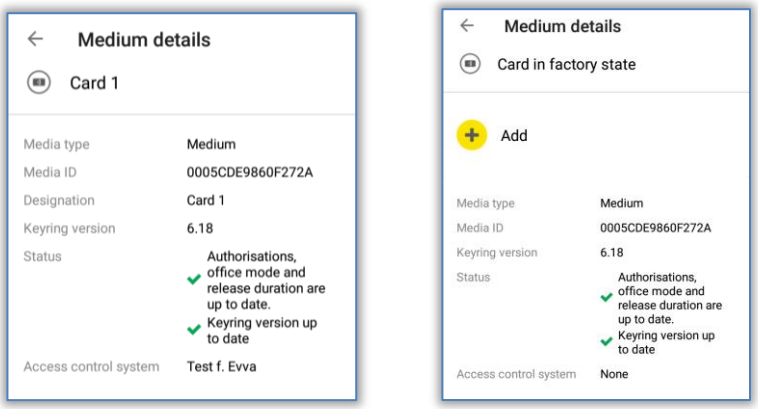
Rys. 251: Symbol "Połącz z komponentem" (tylko w smartfonach Android)

> Postępować zgodnie z instrukcjami i przytrzymać smartfon przy nośniku.

Rys. 252: Aktualizacja danych

Następuje aktualizacja danych. Podczas przesyłania nie wolno odsuwać smartfona od aktualizowanego obiektu. Gdy operacja zostanie zakończona, pojawi się odpowiedni komunikat.

Aby zaktualizować klucz Combi za pomocą smartfona, klucz Combi należy przytrzymać przy smartfonie z tej strony, gdzie znajduje się antena NFC (tam, gdzie widoczny jest symbol RFID).



Rys. 253: Aplikacja AirKey aktualizuje nośnik

Option **Aktualizowanie nośnika za pomocą stacji kodującej**

Aby zaktualizować nośniki (takie jak karty, breloki do kluczy, bransoletki lub klucze Combi) za pomocą stacji kodującej, należy wykonać poniższą procedurę:

Zalogować się do systemu zamknięć AirKey i sprawdzić, czy stacja kodująca została podłączona i wybrana w module zarządzania online.

> Położyć nośnik na stację kodującą.

Rys. 254: Aktualizowanie nośnika za pomocą stacji kodującej

> Usunąć nośnik ze stacji kodującej dopiero wówczas, gdy aktualizacja zostanie pomyślnie zakończona i pojawi się odpowiedni komunikat.

W zależności od tego, czy nośniki znajdują się we własnym lub obcym systemie zamknięć AirKey, wyświetlane informacje komunikatów o pomyślnej realizacji mogą się różnić.

Rys. 255: Własny lub obcy nośnik aktualizowany za pomocą stacji kodującej

Nośniki AirKey należy regularnie aktualizować. Tylko w ten sposób można zapewnić bezpieczeństwo i aktualność danych w systemie AirKey.

Tylko za pomocą regularnej aktualizacji nośników można zapewnić, że wszystkie wpisy do protokołu nośników zostają przesłane do modułu zarządzania online.

Aby wykonać aktualizację klucza Combi za pomocą stacji kodującej, należy położyć na stacji kodującej klucz Combi z tej strony, na której znajduje się symbol RFID. Operacja aktualizacji nie jest możliwa na całym obszarze czytnika stacji kodującej – w przypadku aktualnej wersji (HID Omnikey 5421) klucz Combi będzie wykryty tylko w górnej i dolnej jednej trzeciej czytnika stacji kodującej.

8.4 Aktualizowanie firmware komponentów zamykających

Jeśli dostępny jest nowy firmware dla komponentów zamykających, informacja o tym zostanie wyświetlona w polu szczegółów komponentów zamykających, w zadaniach konserwacyjnych i podczas aktualizacji komponentu zamykającego.

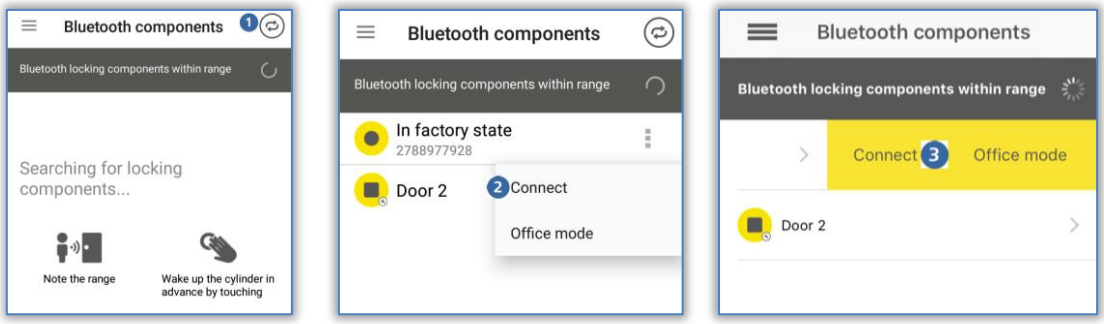
Przed aktualizacją firmware proszę sprawdzić stan baterii w komponencie zamykającym (wkładki). W razie aktywnego ostrzeżenia "Bateria rozładowana" należy najpierw wymienić wszystkie baterie, aby następnie zagwarantować bezbłędną aktualizację.

Bieżąca wersja firmware komponentu zamykającego zostanie wyświetlona w polu "Szczegóły" komponentu.

Aktualizację firmware komponentów zamykających można wykonać za pomocą smartfona lub opcjonalnej stacji kodującej.

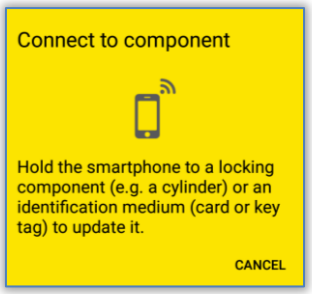
Aby wykonać aktualizację firmware za pomocą smartfona, należy w nim aktywować specjalne uprawnienie "uprawnienie do konserwacji". Aktualizacja firmware za pomocą smartfona odbywa się w następujący sposób:

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.
- Utworzenie połączenia **Bluetooth** (w smartfonach Android): W menu kontekstowym stuknąć komponent zamykający, z którym ma zostać nawiązane połączenie (⋮), a następnie wybrać opcję ***Połącz*** ❷.
- Utworzenie połączenia **Bluetooth** (w iPhone'ach): Przy komponencie zamykającym, z którym ma zostać nawiązane połączenie, przesunąć nazwę komponentu w lewo i wybrać opcję ***Połącz*** ❸.



Rys. 256: Aplikacja AirKey – połączenie z komponentem: Android NFC / Android Bluetooth / iPhone

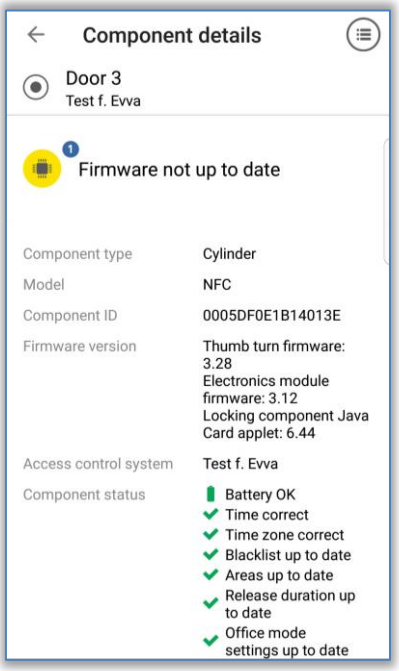
- Postępować zgodnie z instrukcjami.



Rys. 257: Połączenie z komponentem – aktualizacja firmware

Następuje aktualizacja danych. Podczas transmisji nie wolno odsuwać smartfona z funkcją NFC od synchronizowanego komponentu lub ew. nie wolno usuwać smartfona z funkcją Bluetooth z zasięgu komponentu zamykającego. Gdy operacja zostanie zakończona, pojawi się odpowiedni komunikat.

> Komponent zamykający zostanie zaktualizowany i wyświetlą się szczegóły komponentu. W szczegółach komponentu będzie widoczna informacja, że firmware komponentu nie jest aktualny.



Rys. 258: Aplikacja AirKey – szczegóły komponentu

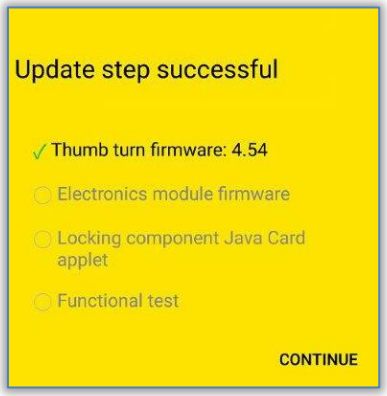
> Na ekranie kliknąć opcję ***Zaktualizuj firmware*** ❶.

> Przytrzymać smartfon z funkcją NFC przy komponencie zamykającym lub pozostać ze smartfonem z funkcją Bluetooth w zasięgu.

Rys. 259: Aplikacja AirKey – aktualizacja firmware

Aktualizacja firmware może w zależności od prędkości połączenia z Internetem trwać do kilku minut. W tym czasie przytrzymać smartfon NFC przy komponencie zamykającym lub w przypadku smartfona z funkcją Bluetooth – pozostać w zasięgu komponentu zamykającego.

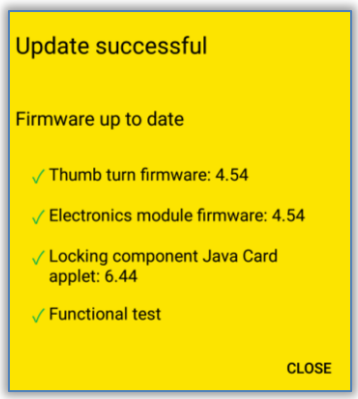
Podczas transmisji nie wolno odsuwać smartfona od aktualizowanego komponentu. Pomyślne wykonanie pierwszego kroku aktualizacji będzie potwierdzone odpowiednim komunikatem.



Rys. 260: Aplikacja AirKey – pomyślne wykonanie procesu w ramach aktualizacji

> Odsunąć smartfon od komponentu zamykającego, aż komponent zamykający zacznie migać i uruchomi sygnalizację akustyczną.
> Przytrzymać smartfon z funkcją NFC przy komponencie zamykającym lub smartfon z funkcją Bluetooth w zasięgu komponentu zamykającego oraz postępować zgodnie z instrukcjami.

Gdy aktualizacja firmware zostanie pomyślnie ukończona, pojawi się odpowiedni komunikat.



Rys. 261: Aplikacja AirKey – pomyślne wykonanie aktualizacji

> Potwierdzić komunikat przyciskiem ***Zamknij***, aby zakończyć aktualizację firmware.

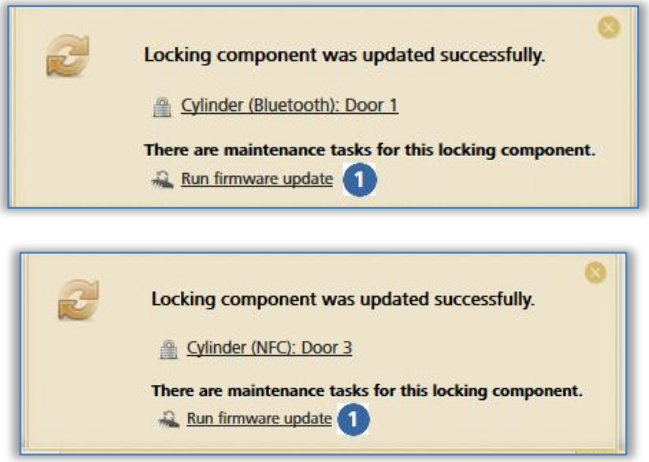
W ten sposób status komponentu zamykającego został ujednolicony w całym systemie. Zadanie konserwacyjne nie będzie już wyświetlane a w szczegółach komponentu zostanie wskazana prawidłowa wersja firmware.

Option

Aktualizowanie firmware za pomocą stacji kodującej:

> Położyć komponent zamykający na stację kodującą. Gdy stacja kodująca nawiąże komunikację z komponentem zamykającym, automatycznie rozpocznie się aktualizacja.

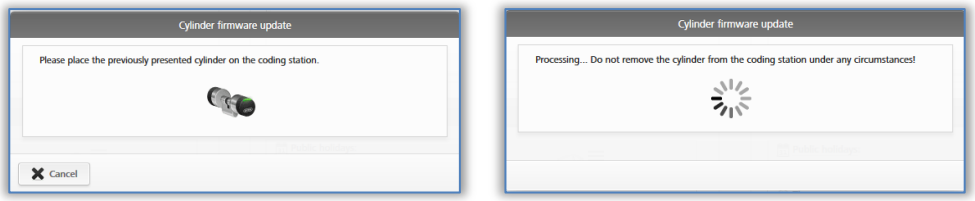
Użytkownik zostanie poinformowany odpowiednim komunikatem o pomyślnym zakończeniu aktualizacji.



Rys. 262: Stacja kodująca – komunikat o pomyślnym zakończeniu aktualizacji

Jeśli będzie dostępna aktualizacja firmware dla komponentu zamykającego, zostanie wyświetlony odpowiedni link ❶.

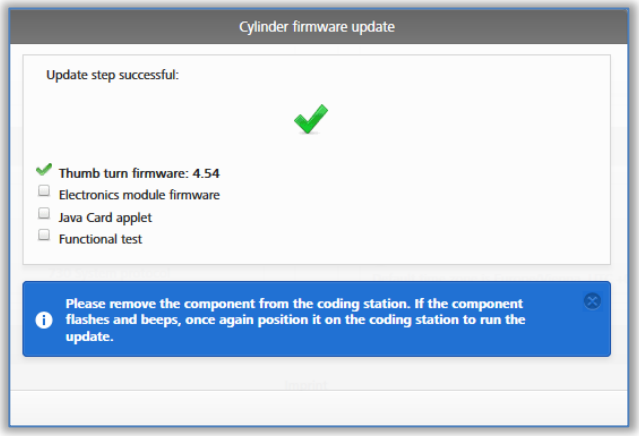
> Kliknąć opcję ***Wykonaj aktualizację firmware***, aby je rozpocząć.



Rys. 263: Stacja kodująca – aktualizacja firmware wkładki AirKey

Aktualizacja firmware może, w zależności od prędkości połączenia z Internetem, trwać do kilku minut. W tym czasie nie wolno oddalać komponentu zamykającego od stacji kodującej.

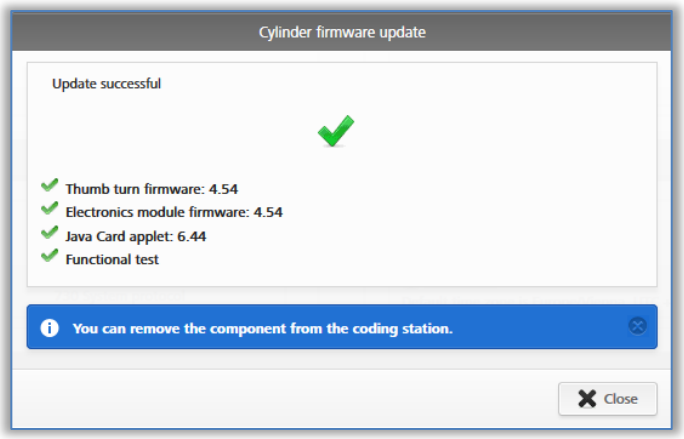
Pierwszy etap aktualizacji firmware będzie potwierdzony odpowiednim komunikatem.



Rys. 264: Stacja kodująca – pomyślne wykonanie etapu aktualizacji

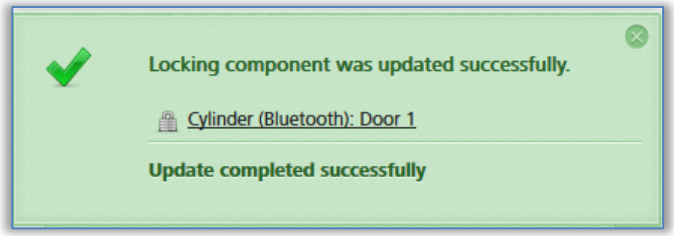
- Zdjąć komponent zamykający ze stacji kodującej, aż komponent wykona ponowne uruchomienie potwierdzone sygnalizacją akustyczną i optyczną.
- Położyć komponent zamykający ponownie na stacji kodującej, aby zakończyć operację.

Gdy aktualizacja zostanie zakończona, pojawi się odpowiedni komunikat.



Rys. 265: Stacja kodująca – pomyślne wykonanie aktualizacji firmware

Komponent zamykający jest aktualizowany jeszcze raz po zamknięciu komunikatu o pomyślnym wykonaniu operacji.



Rys. 266: Stacja kodująca – komponent zamykający został pomyślnie zaktualizowany

> Po aktualizacji usunąć komponent zamykający ze stacji kodującej.

W ten sposób status komponentu zamykającego został ujednolicony w całym systemie. Zadanie konserwacyjne nie będzie już wyświetlane a w szczegółach komponentu zostanie wskazana prawidłowa wersja firmware.

Podczas aktualizacji firmware należy otworzyć drzwi i unieruchomić je, tak aby nie zamknęły się przypadkowo. Następnie przed ponownym zamknięciem drzwi należy sprawdzić, czy komponent zamykający działa prawidłowo.

Podczas aktualizowania firmware komponentów zamykających należy uważać, aby zapewnione było stabilne połączenie z Internetem a połączenie do transferu danych podczas aktualizacji firmware nie zostało przerwane. Do tego celu służą – w zależności od smartfona i systemu operacyjnego – różne ustawienia (np. automatyczny switch sieciowy przełączający pomiędzy mobilnym transferem danych a siecią WLAN).

Firma EVVA zaleca, aby na komponentach zamykających zawsze był zainstalowany firmware w najnowszej wersji.

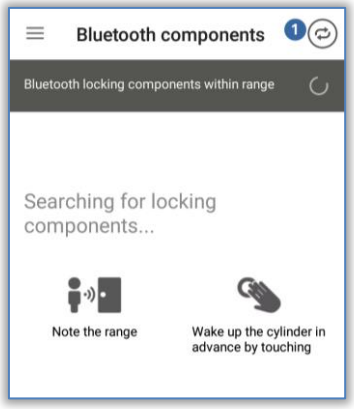
8.5 Aktualizowanie wersji programu Keyring dla nośników

W systemie AirKey "Keyring" jest nazwą programu, który służy do zarządzania wszelkimi danymi istotnymi dla systemu AirKey, zapisanymi na pasywnych nośnikach dostępu, takich jak karty, breloki do kluczy, klucze Combi i bransoletki. Jeśli dostępna jest nowa wersja programu Keyring dla nośników, będzie to wskazane w szczegółach nośników, w zadaniach konserwacyjnych, na stronie startowej ***Home*** oraz podczas aktualizacji nośników.

Bieżąca wersja oprogramowania Keyring nośnika będzie wskazana w szczegółach nośnika.

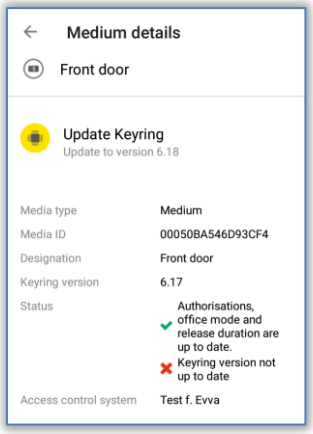
Aktualizację programu Keyring nośników można wykonać za pomocą smartfona lub opcjonalnej stacji kodującej. Aby wykonać aktualizację Keyring za pomocą smartfona, należy w nim aktywować specjalne uprawnienie "uprawnienie do konserwacji". Aktualizacja programu Keyring za pomocą smartfona odbywa się w następujący sposób:

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Nacisnąć symbol ***Połącz z komponentem*** ❶.
- Połączenie ***Bluetooth*** (w smartfonach Android oraz iPhone'ach): W menu głównym aplikacji AirKey wybrać opcję ***Koduj nośniki*** – patrz także rozdział Kodowanie nośników.



Rys. 267: Aplikacja AirKey – połączenie z komponentem

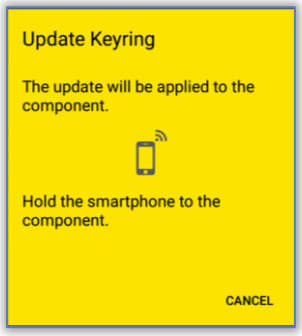
- Przytrzymać smartfon NFC przy nośniku.
- Nośnik zostanie zaktualizowany. Pojawi się informacja o dostępności nowej wersji programu Keyring.



Rys. 268: Aplikacja AirKey – szczegóły nośnika

> Wybrać opcję ***Uaktualnienie programu Keyring***.

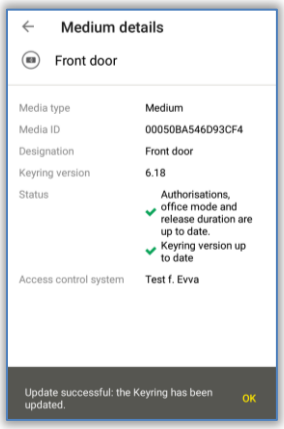
> Przytrzymać smartfon przy nośniku i postępować zgodnie z instrukcjami.



Rys. 269: Aplikacja AirKey – aktualizacja programu Keyring

Aktualizacja programu Keyring może w zależności od prędkości połączenia z Internetem trwać do kilku minut. Przytrzymać smartfon przy nośniku przez wymagany czas.

Podczas przesyłania danych nie wolno odsuwać smartfona od aktualizowanego nośnika. Pomyślne wykonanie aktualizacji programu Keyring będzie potwierdzone odpowiednim komunikatem.



Rys. 270: Aplikacja AirKey – pomyślne wykonanie aktualizacji programu Keyring

W ten sposób status nośnika został ujednolicony w całym systemie. Prawidłowa wersja programu Keyring zostanie wyświetlona w szczegółach nośnika.

Aby wykonać aktualizację klucza Combi za pomocą smartfona, należy przytrzymać przy smartfonie klucz Combi z tej strony, na której znajduje się symbol RFID.

Option **Aktualizowanie wersji programu Keyring za pomocą stacji kodującej:**

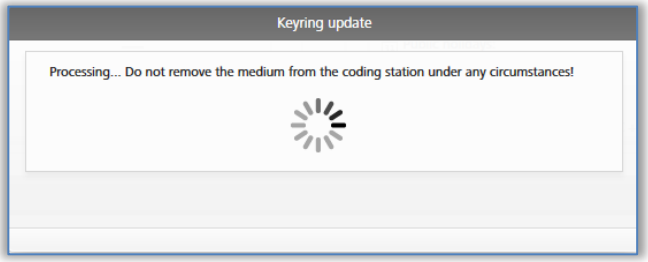
> Położyć nośnik na stację kodującą. Gdy stacja kodująca rozpozna nośnik, zostanie nawiązane połączenie z nośnikiem.

Użytkownik zostanie poinformowany odpowiednim komunikatem o pomyślnym zakończeniu aktualizacji.

Rys. 271: Stacja kodująca – dostępna aktualizacja programu Keyring

Jeśli będzie dostępna aktualizacja Keyring dla nośnika, zostanie wyświetlony odpowiedni link ❶.

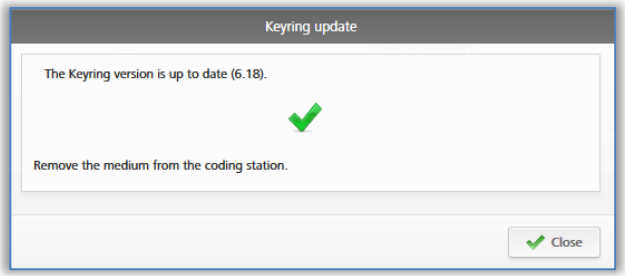
> Kliknąć opcję ***Wykonaj uaktualnienie programu Keyring (x.x)***, aby rozpocząć aktualizację.



Rys. 272: Stacja kodująca – aktualizacja programu Keyring

Aktualizacja wersji programu Keyring może w zależności od prędkości połączenia z Internetem trwać do kilku minut. W tym czasie nie wolno oddalać nośnika od stacji kodującej.

Podczas aktualizacji programu Keyring nie wolno usuwać nośnika ze stacji kodującej. Pomyślna aktualizacja wersji programu Keyring będzie potwierdzona odpowiednim komunikatem.



Rys. 273: Stacja kodująca – pomyślne wykonanie aktualizacji programu Keyring

W ten sposób nastąpiło pomyślne ukończenie aktualizacji programu Keyring. Po zamknięciu komunikatu potwierdzającego nastąpi ponowna aktualizacja nośnika.

Rys. 274: Stacja kodująca – nośnik został pomyślnie zaktualizowany

> Po aktualizacji usunąć nośnik ze stacji kodującej.

Aby wykonać aktualizację klucza Combi za pomocą stacji kodującej, należy położyć na stacji kodującej klucz Combi z tej strony, na której znajduje się symbol RFID. Operacja aktualizacji nie jest możliwa na całym obszarze czytnika stacji kodującej – w przypadku aktualnej wersji (HID Omnikey 5421) klucz Combi będzie wykryty tylko w górnej i dolnej jednej trzeciej czytnika stacji kodującej.

W ten sposób status nośnika został ujednolicony w całym systemie. Prawidłowa wersja programu Keyring zostanie wyświetlona w szczegółach nośnika.

Podczas aktualizowania wersji programu Keyring na nośnikach należy uważać, aby zapewnione było stabilne połączenie z Internetem a połączenie do transferu danych podczas aktualizacji programu Keyring nie zostało rozłączone. Do tego celu służą – w zależności od smartfona lub systemu operacyjnego – różne ustawienia (np. automatyczny switch sieciowy przełączający pomiędzy mobilnym transferem danych a siecią WLAN, unikanie słabych połączeń z Internetem itp.).

Firma EVVA zaleca, aby na nośnikach zawsze była zainstalowana najnowsza wersja programu Keyring.

8.6 Aktualizowanie wersji aplikacji AirKey na smartfonie

Jeśli dostępna jest nowa aplikacja AirKey dla smartfonów, na smartfonie wyświetli się odpowiednia informacja. W zależności od ustawień witryny Google Play Store lub Apple App Store aplikacja AirKey zostanie zaktualizowana automatycznie lub po ręcznym potwierdzeniu.

Po aktualizacji wersji aplikacji AirKey można z niej korzystać tak jak dotychczas.

Do pobrania aplikacji z witryny Google Play Store lub Apple App Store wymagane jest kontro Google lub Apple ID.

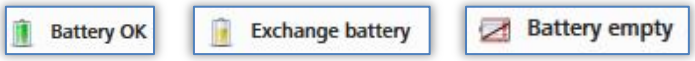
Aktualizacja aplikacji AirKey może być zalecana, ale także pilnie wymagana. W takich przypadkach w aplikacji AirKey pojawi się odpowiedni komunikat. W takiej sytuacji nastąpi ograniczenie niektórych funkcji, ale blokowanie komponentów zamykających będzie możliwe w obydwu przypadkach.

Firma EVVA zaleca, aby na smartfonie zawsze była zainstalowana najnowsza wersja aplikacji AirKey oraz aby została aktywowana opcja automatycznych aktualizacji za pośrednictwem witryny Google Play Store lub Apple App Store.

8.7 Wymiana baterii i otwarcie awaryjne

Komponenty zamykające zasilane baterią wymagają w określonych odstępach czasu wymiany baterii. Stan baterii komponentów zamykających można sprawdzić w Module zarządzania online systemu AirKey oraz podczas aktualizacji komponentu zamykającego za pomocą smartfona z uprawnieniem do konserwacji.

Rozróżnia się trzy różne stany baterii:



Rys. 275: Stan baterii

W razie niskiego stanu naładowania baterii komponent zamykający samodzielnie generuje ostrzeżenie za pomocą specjalnej sygnalizacji w trakcie procesu odryglowania przy użyciu nośnika. Bliższe informacje na temat sygnalizacji można znaleźć w rozdziale Sygnalizacja komponentów zamykających.

8.7.1 Wymiana baterii we wkładce AirKey

Wymianę baterii należy wykonywać przy otwartych i unieruchomionych drzwiach, tak aby nie dopuścić do ich przypadkowego zamknięcia.

Warto pamiętać, że godzina systemowa wkładki AirKey będzie zachowana przez maksymalnie 1 minutę po wyjęciu baterii.

Zdecydowanie zaleca się wykonanie wymiany uszczelek wkładki AirKey w trakcie każdej wymiany baterii, aby zapewnić szczelność elementów. Chodzi tu o uszczelkę pomiędzy trzpieniem gałki i gałką zewnętrzną, a także o uszczelki w tarczy gałki zewnętrznej. Wszystkie te uszczelki są dostępne jako części zamienne. Szczegółowe informacje na ten temat można uzyskać u wyspecjalizowanego sprzedawcy firmy EVVA.

Zdecydowanie zaleca się, aby przynajmniej podczas wymiany baterii nasmarować wkładkę AirKey. W tym celu, po zdjęciu gałki zewnętrznej, należy umieścić kroplę środka smarnego zalecanego przez firmę EVVA pomiędzy trzpieniem gałki a korpusem wkładki od strony zewnętrznej. Dodatkowo, w przypadku tymczasowego demontażu wkładki AirKey, zaleca się nasmarować tylną stronę wkładki pomiędzy zabierakiem a korpusem wkładki. Szczegółowe informacje na ten temat można uzyskać u wyspecjalizowanego sprzedawcy firmy EVVA.

- Wykonać odryglowanie przy komponencie zamykającym za pomocą ważnego nośnika.
- Osadzić narzędzie montażowe, zanim nastąpi ponowne wysprzęglenie wkładki.
- Odkręcić gałkę wkładki za pomocą osadzonego narzędzia montażowego, obracając w kierunku przeciwnym do ruchu wskazówek zegara.
- Zdjąć narzędzie montażowe z gałki.
- Otworzyć gałkę, odkręcając trzy śruby na tylnej stronie gałki.
- Wyjąć tarczę gałki.
- Ostrożnie poluzować uchwyt na baterie, przemieszczając go do góry.
- Wymienić baterię. Sprawić, czy bateria została zamocowana w prawidłowej pozycji. Nie należy przy tym łączyć starych i nowych baterii.
- Ostrożnie zamocować uchwyt na baterie.
- Osadzić tarczę gałki w gałce. Przymocować gałkę za pomocą trzech śrub.
- Osadzić narzędzie montażowe na gałce.
- Upewnić się, że pierścień uszczelniający na trzpieniu wkładki został prawidłowo osadzony i ponownie umieścić gałkę nad wkładką, obracając zgodnie z ruchem wskazówek zegara, aż do wyczuwalnego oporu.
- Zdjąć narzędzie montażowe.
- Obrócić gałkę w kierunku przeciwnym do ruchu wskazówek zegara, aż się zauważalnie zatrzaśnie.
- Upewnić się, że gałka i moduł elektroniczny zostały prawidłowo zatrzaśnięte.
- Następnie należy zaktualizować wkładkę za pomocą smartfona lub stacji kodującej, aby przesłać aktualne wpisy do protokołu do Modułu zarządzania online systemu AirKey.
- Przed zamknięciem drzwi sprawdzić działanie wkładki za pomocą próbnego odryglowania.

Z uwagi na fizyczne właściwości baterii, w przypadku utrzymujących się przez dłuższy czas niskich temperatur (poniżej -10 °C), baterie należy wcześniej wymieniać i bacznie obserwować działanie oraz stan baterii.

Jeśli po wymieni baterii zostanie zasygnalizowany błąd komunikacji, będzie to wynikać z próby nawiązania komunikacji między gałką a modułem elektronicznym. Nie będzie ona funkcjonować, jeśli gałka nie została przyśrubowana na module elektronicznym.

Stan baterii komponentów zamykających należy sprawdzać za pomocą smartfona z uprawnieniem do konserwacji, wykonując aktualizację komponentu zamykającego. Następnie można przejrzeć szczegóły komponentu zamykającego.

Jeśli zdarzy się, że baterie nie zostały w porę wymienione, istnieje możliwość otwarcia awaryjnego za pomocą opcjonalnego zasilacza awaryjnego.

Opis procedury znajduje się w rozdziale Zasilacz awaryjny.

Po otwarciu awaryjnym należy wymienić baterie i wykonać aktualizację komponentu zamykającego przed ponownym zamknięciem drzwi.

Po użyciu należy starannie założyć białą osłonę gumową z logo EVVA, aby zabezpieczyć otwór gniazda do podłączenia zasilacza awaryjnego przed wnikaniem pyłu i wilgoci. Do tego celu nie należy stosować ostrych przedmiotów, aby uniknąć możliwych uszkodzeń.

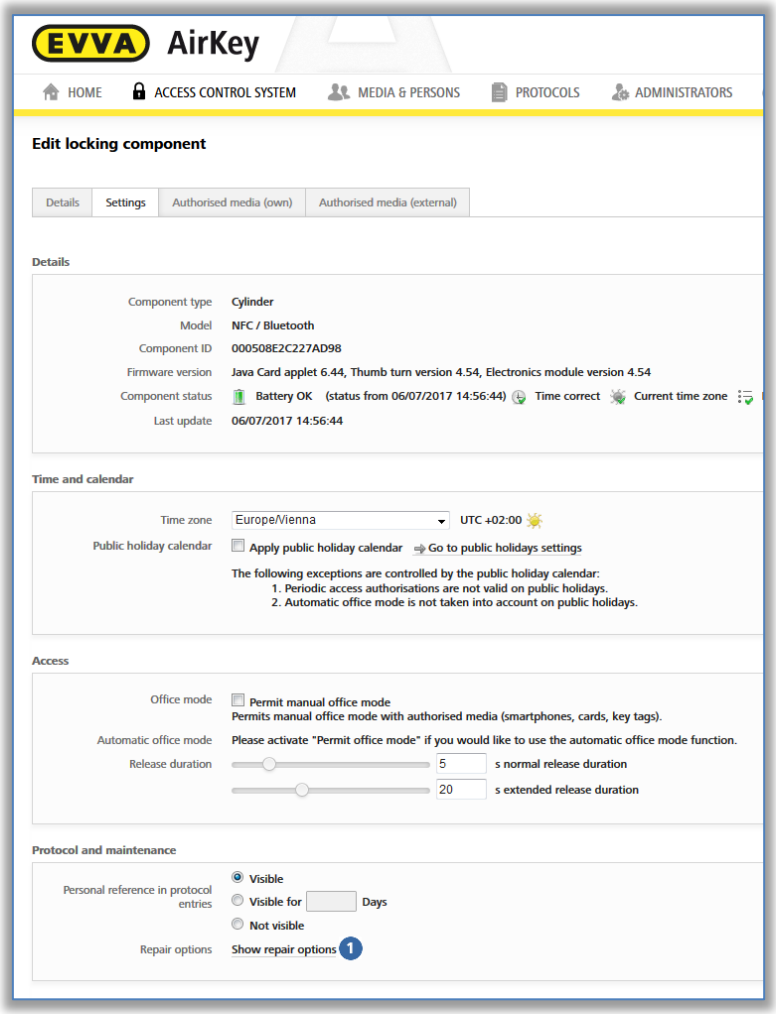
8.8 Opcje naprawy

Opcje naprawy komponentów zamykających umożliwiają reagowanie w przypadku usterki tych komponentów. Istnieje możliwość utworzenia zamiennego komponentu zamykającego w systemie zamknięć lub usunięcia uszkodzonego komponentu zamykającego z systemu.

8.8.1 Utworzenie i montaż zamiennego komponentu zamykającego

Podczas tworzenia i późniejszego montażu komponentu zamiennego następuje zamiana istniejącego, uszkodzonego komponentu na komponent zamykający w stanie fabrycznym. Jednocześnie wszystkie parametry, a także uprawnienia dla tego komponentu w systemie AirKey zostają zachowane. Po wykonaniu operacji zamienny komponent zamykający nie będzie już w stanie fabrycznym.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście przeglądu kliknąć ten komponent zamykający, który będzie edytowany.
- W zakładce "Ustawienia" w bloku ***Protokołowanie i konserwacja*** kliknąć ***Wyświetl opcje naprawy*** ℹ.

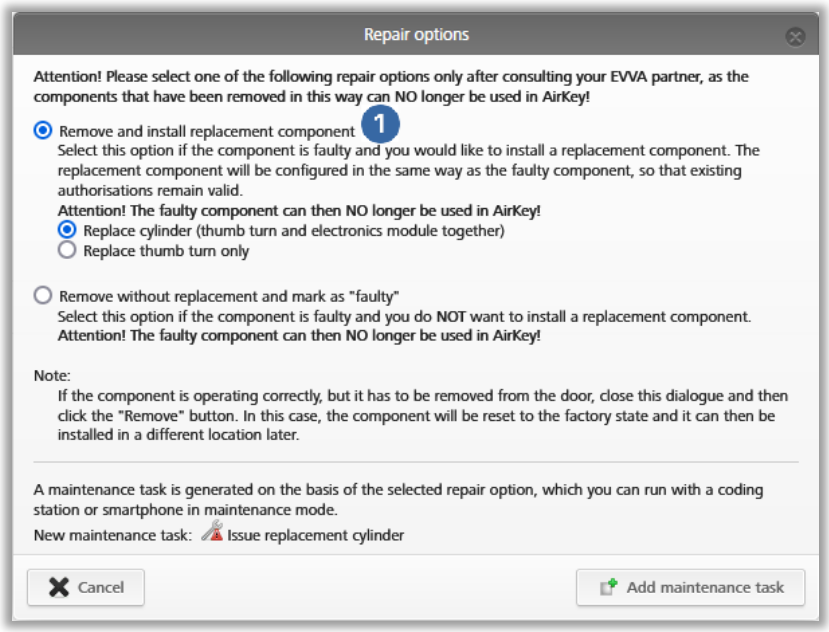


Rys. 276: Edycja komponentu zamykającego – opcje naprawy

Otworzy się okno dialogowe ***Opcje naprawy***.

> Standardowo wstępnie ustawiono przyciski ***Zdemontuj i zainstaluj komponenty zamienne*** ❶ oraz ***Wymień wkładkę (gałkę i moduł elektroniczny razem)***.

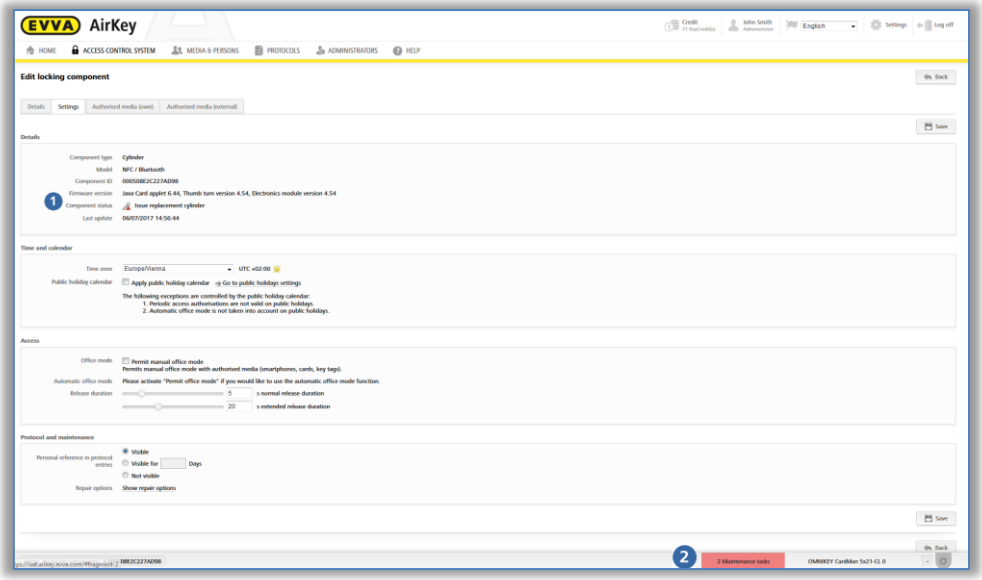
> Alternatywnie można też wybrać przycisk ***Wymień wyłącznie gałkę***.



Rys. 277: Opcje naprawy

> Kliknąć opcję ***Dodaj zadanie konserwacyjne***.

Stan komponentu zamykającego ❶ zostanie zaktualizowany i wyświetlony jako zadanie konserwacyjne ❷.



Rys. 278: Status komponentu i zadanie konserwacyjne

W ten sposób przygotowanie do utworzenia i montażu zamiennego komponentu zamykającego w ramach Modułu zarządzania online systemu AirKey zastanie ukończone. Aby w pełni zakończyć procedurę, należy jeszcze utworzyć i zamontować komponent zamienny za pomocą smartfona z uprawnieniem do konserwacji lub opcjonalnej stacji kodującej.

Zamieniany komponent można nadal aktualizować – aż do momentu kompletnego ukończenia montażu komponentu zamiennego. Aby zapewnić kompletność protokołów, należy jeszcze zamontować dostępy między kom-

ponentem zamiennym oraz pomyślnie zatwierdzić komponent zamienny.

W razie wymiany komponentów zamykających Bluetooth zarówno zamieniony, jak i zamienny komponent będzie uwzględniony na liście komponentów Bluetooth w zasięgu. Wymieniony komponent należy po przeprowadzonej wymianie odłączyć od prądu, dopiero wówczas zniknie on z listy komponentów Bluetooth.

Utworzenie i montaż zamiennego komponentu zamykającego za pomocą smartfona

Warunkiem niezbędnym jest smartfon z uprawnieniem do konserwacji dla tego systemu zamknięć, w którym ma nastąpić utworzenie i montaż zamiennego komponentu zamykającego.

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Stuknąć symbol ***Połącz z komponentem*** i przytrzymać smartfon przy komponencie zamykającym w stanie fabrycznym.
- Utworzenie połączenia **Bluetooth** (w smartfonach z systemem **Android**): W menu kontekstowym wybrać komponent zamykający w stanie fabrycznym, który ma być dodany do systemu zamknięć (⋮), a następnie wybrać opcję ***Połącz***.
- Utworzenie połączenia **Bluetooth** (w urządzeniach **iPhone**): Przesunąć komponent zamykający w stanie fabrycznym, który ma być dodany do systemu zamknięć i który ma oznaczenie "W stanie fabrycznym", w lewo, a następnie wybrać opcję ***Połącz***.
- Po aktualizacji, w polu szczegółów komponentu zamykającego kliknąć opcję ***Utwórz wkładkę zamienną***.
- W następnym oknie dialogowym stuknąć komponent zamykający, który ma zostać zamieniony i potwierdzić przyciskiem ***Dalej***.
- W razie połączenia NFC należy ponownie przytrzymać smartfon przy komponencie zamykającym w stanie fabrycznym. W razie połączenia Bluetooth należy wybrać komponent zamykający w stanie fabrycznym z listy komponentów zamykających będących w zasięgu.
- Potwierdzić, czy ma zostać utworzone zadanie konserwacyjne do późniejszego montażu.
- Zakończyć procedurę przyciskiem ***Zamontuj później***, jeśli komponent zamykający musi być jeszcze zamontowany w drzwiach, lub przyciskiem ***Zakończ***, jeśli montaż w drzwiach został już wykonany.
- Wykonać aktualizację komponentu zamykającego po montażu w drzwiach.

Option Utworzenie i montaż zamiennego komponentu zamykającego za pomocą stacji kodującej.

- Położyć zamienny komponent zamykający w stanie fabrycznym na stacji kodującej.
- W prawej, dolnej części okna dialogowego wybrać opcję ***Utwórz wkładkę zamienną*** oraz ten komponent zamykający, który ma zostać wymieniony.

Rys. 279: Komponent w stanie fabrycznym – utworzenie wkładki zamiennej

- Kliknąć przycisk ***Dalej***.
- Położyć zamienny komponent zamykający w stanie fabrycznym na stacji kodującej.
- Komponent zamienny należy odsunąć dopiero wówczas, gdy pojawi się odpowiedni komunikat o pomyślnym wykonaniu operacji.
- Potwierdzić, czy ma zostać utworzone zadanie konserwacyjne do późniejszego montażu.
- Zakończyć procedurę przyciskiem ***Zamontuj później***, jeśli komponent zamykający musi być jeszcze zamontowany w drzwiach, lub przyciskiem ***Zakończ***, jeśli montaż w drzwiach został już wykonany.
- Wykonać aktualizację komponentu zamykającego po montażu w drzwiach.

Jeśli zamienny komponent zamykający ma starą wersję firmware, aktualizacja firmware będzie wykonana podczas tego procesu.

Zamieniony komponent zamykający po tej operacji nie będzie nadawał się do użytku. Dlatego tę funkcję należy wykonywać tylko wówczas, gdy komponent zamykający jest rzeczywiście uszkodzony i nie będzie już potrzebny.

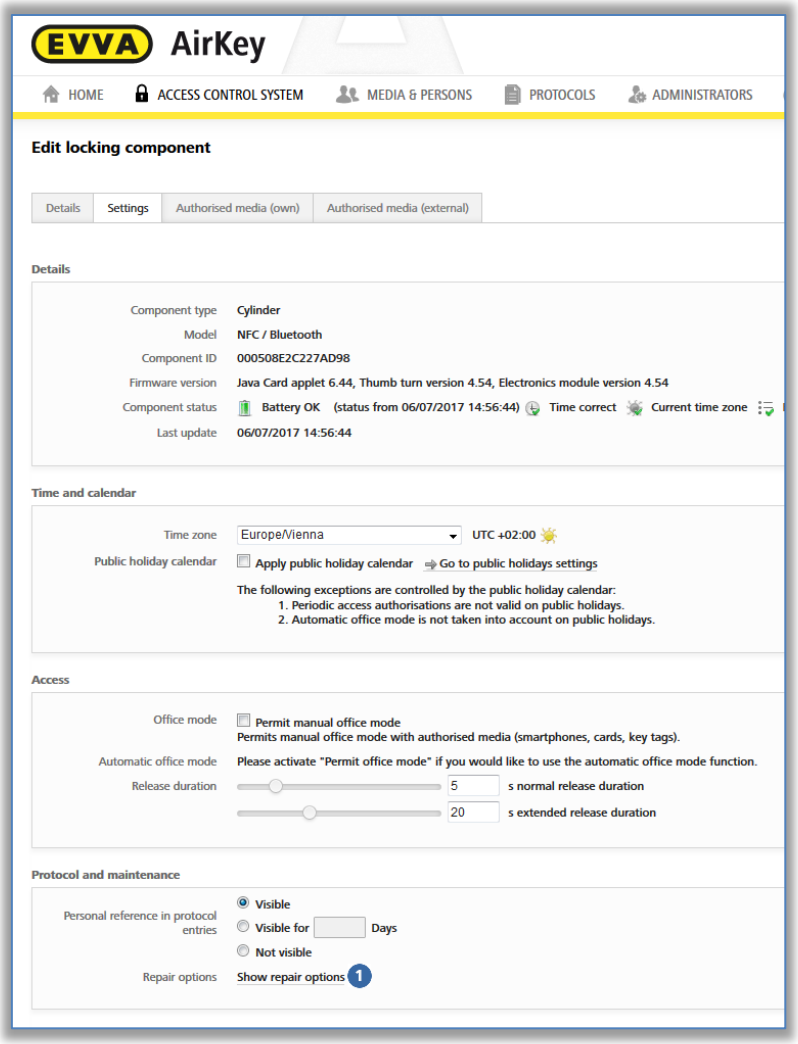
8.8.2 Demontaż komponentu zamykającego bez montowania zamiennika i oznaczenie jako element "uszkodzony"

Jeśli uszkodzony komponent zamykający nie musi być wymieniony, ale mimo to już nie powinien być uwzględniany w systemie, można go przy użyciu opcji naprawy zdemontować bez zamiennika.

W tak przypadku późniejsza aktualizacja komponentu zamykającego nie będzie możliwa, a przez to komponent będzie bezużyteczny.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście przeglądu kliknąć ten komponent zamykający, który będzie edytowany.

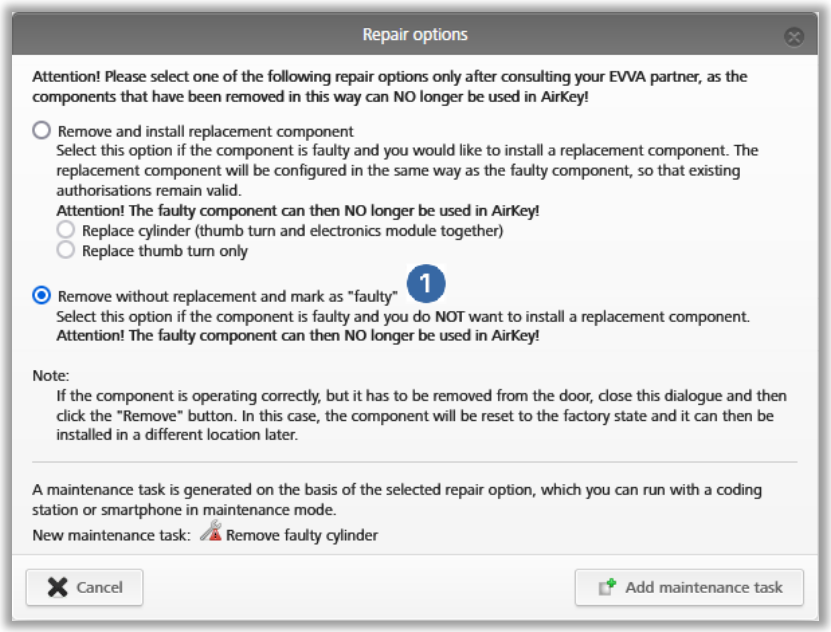
> W zakładce ***Ustawienia*** w bloku ***Protokołowanie i konserwacja*** kliknąć link ***Wyświetl opcje naprawy*** ❶.



Rys. 280: Edycja komponentu zamykającego – opcje naprawy

Otworzy się okno dialogowe "Opcje naprawy".

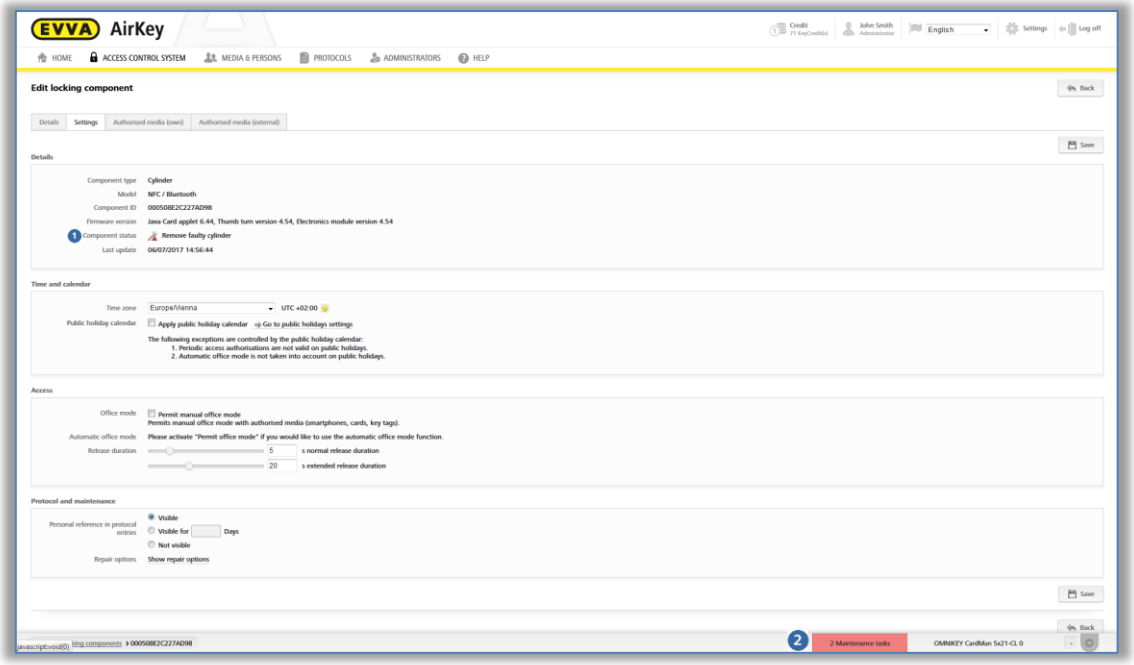
> Wybrać opcję ***Zdemonuj bez zamiennika i zaznacz jako "uszkodzona"*** ❶.



Rys. 281: Opcje naprawy

> Kliknąć opcję ***Dodaj zadanie konserwacyjne***.

Stan komponentu zamykającego ❶ zostanie zaktualizowany i wyświetlony jako zadanie konserwacyjne ❷.



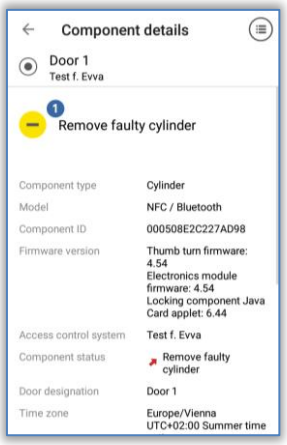
Rys. 282: Status komponentu i zadanie konserwacyjne

W ten sposób przygotowanie do demontażu komponentu zamykającego bez zamiennika w ramach Modułu zarządzania online systemu AirKey zastanie ukończone. Aby w pełni zakończyć procedurę, demontaż należy ukończyć przy użyciu smartfona z uprawnieniem do konserwacji lub Modułu zarządzania online systemu AirKey.

8.8.3 Demontaż uszkodzonego komponentu zamykającego przy użyciu smartfona

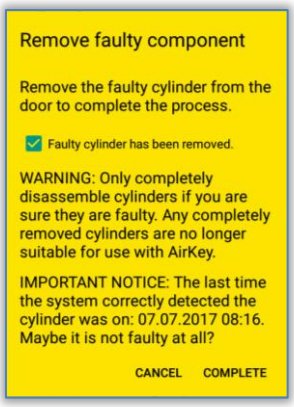
Jeśli aktualizacja uszkodzonego komponentu zamykającego jest jeszcze możliwa, można wykonać demontaż uszkodzonego komponentu zamykającego bez zamiennika przy użyciu smartfona. Konieczny jest zarejestrowany smartfon z aktywnym uprawnieniem do konserwacji dla danego systemu zamknięć AirKey.

- Utworzenie połączenia **NFC** (w smartfonach z systemem Android): Stuknąć symbol ***Połącz z komponentem*** i przytrzymać smartfon przy komponencie zamykającym, który ma zostać zdemontowany.
- Utworzenie połączenia **Bluetooth** (w smartfonach z systemem **Android**): W menu kontekstowym stuknąć komponent zamykający, który ma zostać zdemontowany (⋮), a następnie wybrać opcję ***Połącz***.
- Utworzenie połączenia **Bluetooth** (w urządzeniach **iPhone**): Przy komponencie zamykającym, który ma zostać zdemontowany, przesunąć nazwę komponentu w lewo i wybrać opcję ***Połącz***.
- Zostaną wyświetlone szczegóły komponentu. Wybrać opcję ***Wymontuj uszkodzoną wkładkę*** ❶.



Rys. 283: Smartfon – demontaż uszkodzonego komponentu

- Zaznaczyć pole wyboru w oknie dialogowym i potwierdzić przyciskiem ***Zakończ***.



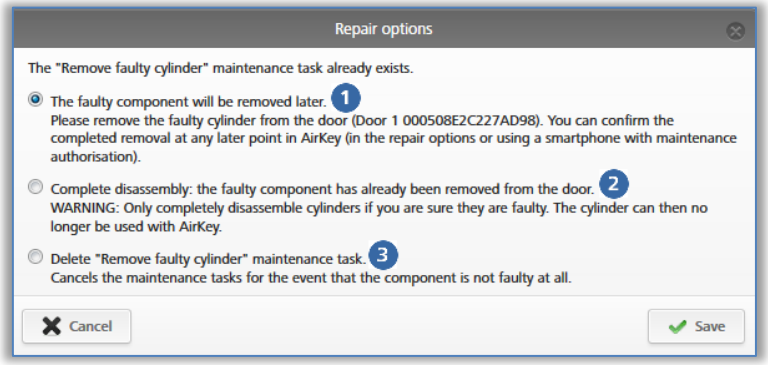
Rys. 284: Smartfon – demontaż uszkodzonego komponentu – potwierdzenie

W ten sposób następuje zakończenie procedury i komponent zamykający nie będzie już wyświetlany w systemie zamknięć AirKey. Teraz komponent zamykający nie nadaje się do użytku.

8.8.4 Demontaż uszkodzonego komponentu zamykającego przy użyciu modułu zarządzania online

Jeśli komponentu zamykającego z powodu uszkodzenia nie można więcej aktualizować, demontaż bez zamiennika należy wykonać poprzez Moduł zarządzania online systemu AirKey.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny*** – w zależności od tego, który komponent został oznaczony jako uszkodzony.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście przeglądu kliknąć komponent zamykający, który będzie edytowany.
- W zakładce ***Ustawienia*** w bloku ***Protokołowanie i konserwacja*** kliknąć link ***Wyświetl opcje naprawy***.
- Pojawi się okno dialogowe z trzema możliwościami wyboru.



Rys. 285: Demontaż uszkodzonego komponentu zamykającego

- W przypadku opcji ***Uszkodzony komponent zostanie później wymontowany*** ❶ nastąpi zachowanie aktualnego statusu komponentu i komponent zamykający nadal pozostanie częścią systemu zamknięć AirKey.

- W przypadku opcji ***Wykonanie demontażu: Uszkodzony komponent został już wymontowany z drzwi*** ❷ nastąpi proces bezzamiennikowego demontażu uszkodzonego komponentu zamykającego i komponent zamykający został usunięty z systemu AirKey.

- W przypadku opcji ***Usuń zadanie konserwacyjne "Demontuj uszkodzoną wkładkę"*** ❸ nastąpi anulowanie demontażu bezzamiennikowego. Bliższe informacje można znaleźć w rozdziale Anulowanie zadań konserwacyjnych w przypadku opcji naprawy.

Komponent zamykający, który został zdemontowany bez zamiennika, nie będzie nadawał się do użycia po tej operacji. Dlatego tę funkcję należy wykonywać tylko wówczas, gdy komponent zamykający jest rzeczywiście uszkodzony i nie będzie już potrzebny.

Jeśli użytkownik chce usunąć działający komponent zamykający ze swojego systemu zamknięć, należy skorzystać z instrukcji zawartych w rozdziale Usuwanie komponentu zamykającego.

8.8.5 Anulowanie zadań konserwacyjnych w przypadku opcji naprawy

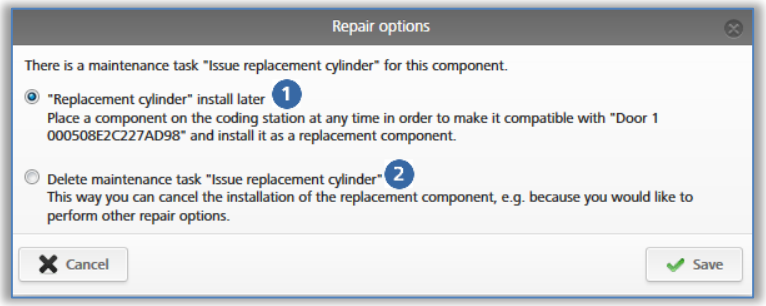
Jeśli omyłkowo utworzono zadanie konserwacyjne dla zamiennego komponentu zamykającego lub demontażu bez zamiennika, można je w późniejszym czasie usunąć.

> Na stronie startowej ***Home*** kliknąć link ***Zadania konserwacyjne***.

> Wybrać z listy żądane zadanie konserwacyjne.

> W zakładce ***Ustawienia*** w bloku ***Protokołowanie i konserwacja*** kliknąć link ***Wyświetl opcje naprawy***.

> Wybrać w zależności od otwartego zadania konserwacyjnego, czy zamienny komponent zamykający (wkładka, gałka, czytnik naścienny) powinien zostać później utworzony ❶ lub czy zadanie konserwacyjne ma zostać usunięte ❷.



Rys. 286: Usuwanie zadania konserwacyjnego

> Kliknąć przycisk ***Przejmij***.

W ten sposób zadanie konserwacyjne zostaje anulowane. Stan komponentu zamykającego zostanie zaktualizowany zgodnie z ostatnim stanem komponent.

Jeśli zadanie konserwacyjne opcji naprawy zostało już wykonane, nie można go już anulować.

Należy korzystać z tej funkcji w celu anulowania zadania konserwacyjnego "Komponent musi zostać usunięty" także wówczas, gdy nieuszkodzony komponent zamykający został usunięty z systemu zamknięć AirKey.

9 Nośniki awaryjne

Nośnik awaryjny to nośnik o nieograniczonej dacie ważności, z uprawnieniem dostępu do wszystkich komponentów zamykających w systemie zamknięć AirKey. Nośniki awaryjne stosuje się w sytuacjach wyjątkowych (np. podczas akcji straży pożarnej) i należy je przechowywać w bezpiecznym miejscu. Nośniki awaryjne zachowują uprawnienie dostępu do komponentu zamykającego bez ograniczenia czasowego. Należy jedynie zapewnić zasilanie elektrycznego dla komponentów zamykających.

9.1 Utworzenie nośników awaryjnych

W celu utworzenia nośnika awaryjnego należy położyć nośnik w postaci karty, breloka do kluczy lub karty Combi – zgodnie z opisem w rozdziale Utworzenie karty, breloka do kluczy lub klucza Combi – oraz przydzielić nośnikom awaryjnym uprawnienia stałego dostępu do wszystkich drzwi w ramach systemu zamknięć. Należy pamiętać o odpowiedniej aktualizacji nośników awaryjnych w razie rozbudowy systemu, aby zapewnić dostęp do dodatkowych drzwi w nagłym przypadku. Nośniki awaryjne mają także dostęp do komponentów zamykających z nieprawidłową godziną (np. wkładki mogą utracić zapis godziny, gdy baterie rozładują się). Informacje na temat przekazywania i potwierdzania uprawnień można znaleźć w rozdziałach Przydzielanie uprawnień i Potwierdzenie uprawnienia.

Warto pamiętać, że również nośniki w postaci kart, breloków do kluczy, bransoletki lub kluczy Combi mogą ulec uszkodzeniu. Dlatego w zależności od systemu zamknięć należy utworzyć odpowiednią liczbę nośników awaryjnych.

Zalecane nośniki awaryjne to karty, breloki do kluczy, bransoletki oraz klucze Combi, ponieważ smartfony z uwagi na ograniczony czas pracy akumulatorów nie nadają się do tego celu.

Aby ułatwić zarządzanie nośnika awaryjnymi, można utworzyć strefy, które zawierają wszystkie drzwi wchodzące w skład systemu zamknięć. Następnie należy przypisać do nośników awaryjnych nieograniczone uprawnienie do stałego dostępu dla tej strefy.

10 Praca z kilkoma systemami zamknięć AirKey

W poniższym rozdziale zawarto wskazówki dotyczące pracy z kilkom systemami zamknięć AirKey.

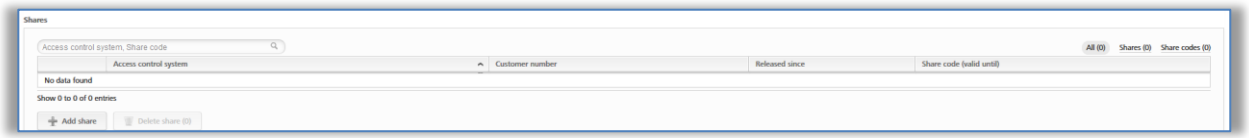
10.1 Udostępnianie komponentu zamykającego do innego systemu zamknięć

Komponenty w swoim systemie zamknięć można udostępnić do użytkowania w ramach innego systemu. Wówczas także zarządzanie uprawnieniami dla tego komponentu zamykającego odbywa się poprzez inny system zamknięć. Każdy komponent zamykający można udostępnić maksymalnie do 250 systemów.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście przeglądu kliknąć oznaczenie drzwi tego komponentu zamykającego, który będzie udostępniany.

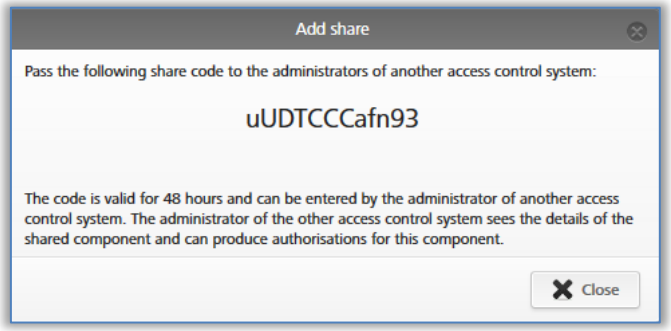
W bloku ***Zezwolenia*** w szczegółach komponentu zamykającego znajduje się wyszczególnienie już udzielonych udostępnień.

- Kliknąć opcję ***Dodaj zezwolenie***.



Rys. 287: Udostępnianie komponentu zamykającego

- Zostanie wygenerowany 12-znakowy kod zezwolenia.



Rys. 288: Dodawanie zezwolenia

- Przekazać kod zezwolenia administratorowi innego systemu zamknięć.

Kod zezwolenia zachowuje ważność przez 48 godzin.

Dla jednego komponentu zamykającego można wygenerować więcej kodów zezwoleń. Są one wyświetlane na liście zezwoleń komponentu zamykającego.

Zostanie utworzona pozycja na liście zezwoleń komponentu zamykającego. Można z niej odczytać kod zezwolenia i jego okres ważności.

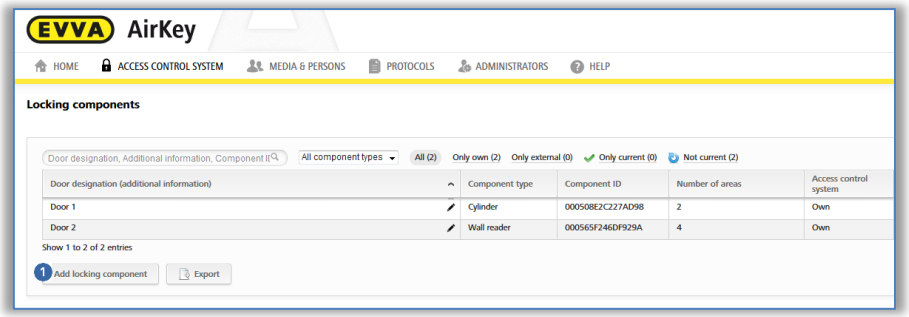
10.2 Dodawanie komponentu zamykającego z innego systemu zamknięć

Jeśli do własnego systemu udostępniony został komponent zamykający z innego systemu zamknięć, należy dodać go do własnego systemu zamknięć.

> Na stronie startowej ***Home*** na szarym pasku ***System zamknięć*** kliknąć opcję ***Dodaj*** → ***Dodaj komponent zamykający*** ❶.

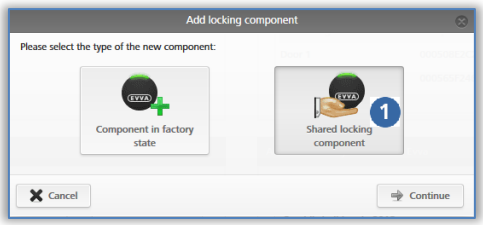
Rys. 289: Dodawanie komponentu zamykającego – szary pasek

> Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
> Kliknąć opcję ***Dodaj komponent zamykający*** ❶.



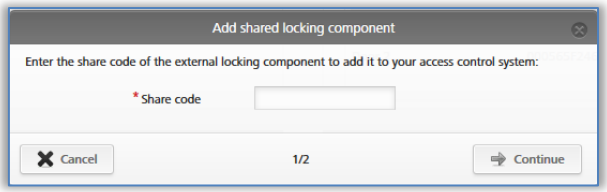
Rys. 290: Dodawanie komponentu zamykającego

> Jako rodzaj należy wybrać ***Udostępniony komponent zamykający*** ❶.
> Kliknąć przycisk ***Dalej***.



Rys. 291: Dodawanie udostępnionego komponentu zamykającego

> Wprowadzić kod zezwolenia innego systemu zamknięć w celu dodania komponentu zamykającego.



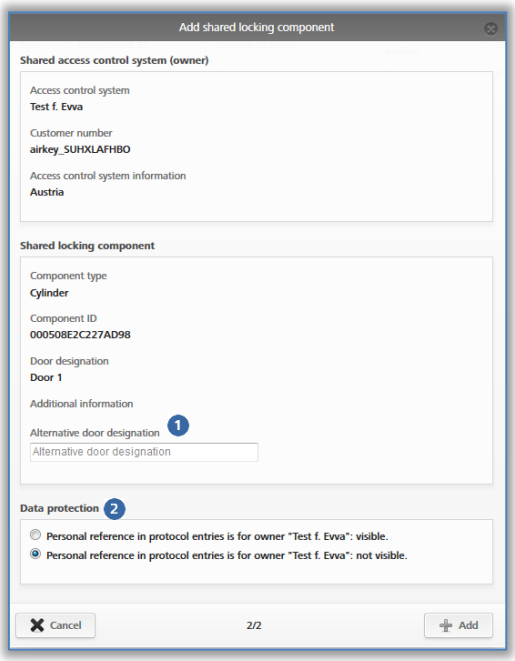
Rys. 292: Dodawanie udostępnionego komponentu zamykającego

Jeśli wprowadzony kod zezwolenia jest nieprawidłowy, zostanie wyświetlony komunikat błędu.

Jeśli wprowadzony kod zezwolenia jest prawidłowy, będzie możliwe przyjęcie następujących ustawień:

> Alternatywne oznaczenie drzwi ❶.

> Ze względu na ochronę danych relacje osobowe we wpisach do protokołu mogą być widoczne lub niewidoczne ❷ dla właścicieli komponentu zamykającego.



Rys. 293: Dodawanie udostępnionego komponentu zamykającego

> Zostanie utworzone zadanie konserwacyjne.

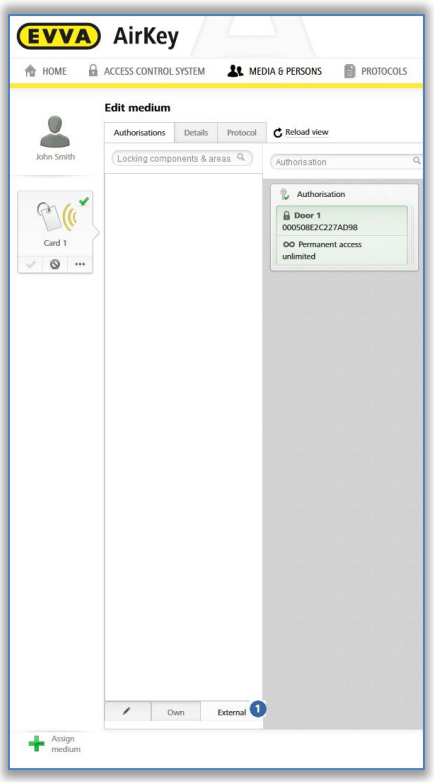
- Zaktualizować komponent zamykający za pomocą smartfona z uprawnieniem do konserwacji lub opcjonalnej stacji kodującej.
- W ten sposób zadanie konserwacyjne zostanie usunięte z listy i zezwolenie będzie aktualne.
- Gdy udostępniony komponent zamykający zostanie dodany, odpowiednia pozycja pojawi się na liście komponentów zamykających w kolumnie "System zamknięć" z atrybutem "nieznane". Ten klient, który dodał komponent zamykający, może w zakładce "Szczegóły" wprowadzić alternatywne oznaczenie drzwi oraz przypisać komponent do strefy. W zakładce "Ustawienia" można w bloku "Ochrona danych" zmienić ustawienia przycisków, tak aby rozróżnić relacje osobowe we wpisach do protokołu pomiędzy możliwością przeglądu i brakiem możliwości przegląd dla właścicieli komponentu zamykającego. Ponadto relację osobową we wpisach do protokołu można ustawić w bloku "Protokołowanie i konserwacja" dla udostępnionego systemu zamknięć. Oprócz tego można przydzielić uprawnienia dostępu dla udostępnionego komponentu zamykającego.

Obcego komponentu zamykającego nie można udostępniać do innego systemu zamknięć.

10.3 Przydzielanie uprawnień do udostępnionego komponentu zamykającego

W tym systemie zamknięć AirKey, do którego dodano udostępniony komponent zamykający, procedura przydzielania uprawnień różni się nieznacznie od procedury właściciela komponentu zamykającego. Jeśli udostępniony komponent zamykający dodano do systemu zamknięć, należy wykonać poniższe czynności.

- Na stronie startowej ***Home*** wybrać ikonę ***Smartfony*** lub ***Karty***.
- Alternatywnie w menu głównym wybrać ***Nośniki i osoby*** → ***Nośniki***.
- Na liście przeglądu kliknąć żądany nośnik.
- Jeśli nośnik został przypisany do osoby, pojawi się przegląd uprawnień nośnika.
- Poniżej ikon wszystkich komponentów zamykających i stref wybrać zakładkę ***Nieznane*** ❶, aby wyświetlić wszystkie dodane komponenty zamykające obcych systemów zamknięć.



Rys. 294: Uprawnienie dla udostępnionego komponentu zamykającego

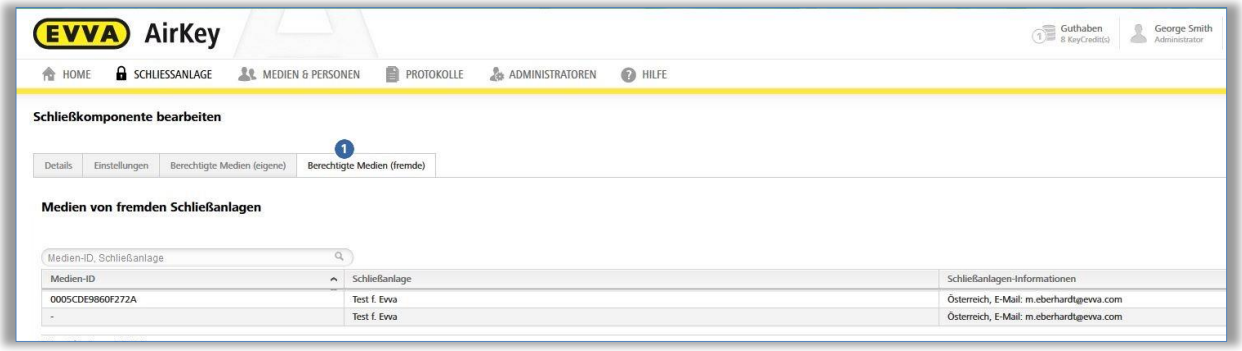
- Przeciągnąć przycisk z wybranymi udostępnionymi drzwiami metodą "przeciągnij i upuść" na szare pole. Dopiero po przesunięciu wybranych drzwi / wybranej strefy na środkowe pole zostaną wyświetlone rodzaje dostępu.
- Wybrać żądany rodzaj dostępu, przeciągając wybrane drzwi / wybraną strefę metodą "przeciągnij i upuść" na odpowiednie pole.
- Potwierdzić uprawnienie, aby wyksięgować jedną jednostkę KeyCredit. Bliższe informacje na temat potwierdzania uprawnień można znaleźć w rozdziale Potwierdzanie uprawnienia. Jednostka KeyCredit zostanie pobrana z konta własnego systemu zamknięć, a nie z konta innego systemu.

10.4 Przeglądanie uprawnień do udostępnionego komponentu zamykającego

Jeśli użytkownik udostępnił komponent zamykający innemu klientowi, można także przeglądać nośniki innego klienta, które są uprawnione do udostępnionego komponentu zamykającego.

- Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.
- Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.
- Na liście przeglądu kliknąć ten komponent zamykający, którego szczegóły mają być wyświetlone.

> Kliknąć opcję ***Uprawnione nośniki (nieznane)*** ❶, aby wyświetlić przegląd wszystkich obcych nośników, które mają uprawnienia dla danego komponentu zamykającego.



Rys. 295: Uprawnione nośniki (nieznane)

10.5 Anulowanie udostępnienia komponentu zamykającego

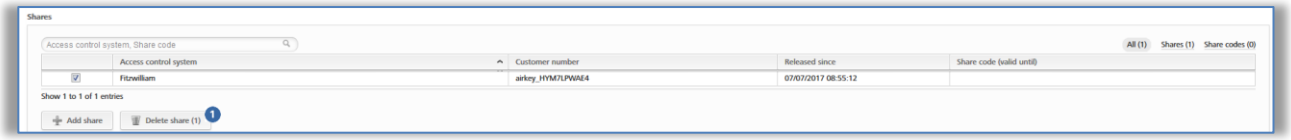
Istnieje możliwość anulowania przyznanego udostępnienia komponentu zamykającego. W tym celu należy wykonać następującą procedurę:

> Na stronie startowej ***Home*** wybrać ikonę ***Wkładka*** lub ***Czytnik naścienny***.

> Alternatywnie wybrać w menu głównym opcje ***System zamknięć*** → ***Elementy zamykające***.

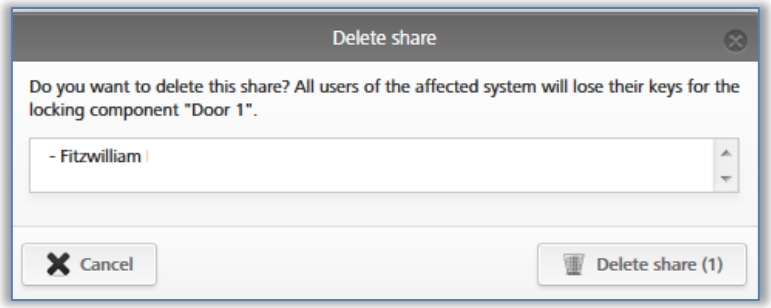
> Na liście przeglądu kliknąć pozycję komponentu zamykającego, którego udostępnienie zostanie anulowane.

W zakładce ***Szczegóły*** w bloku ***Zezwolenia*** wybrać odpowiednie zezwolenie i kliknąć opcję ***Kasuj zezwolenie*** ❶.



Rys. 296: Blok "Zezwolenia" – kasowanie zezwolenia

> Potwierdzić pytanie bezpieczeństwa przyciskiem ***Kasuj zezwolenie***.



Rys. 297: Kasowanie zezwolenia

W ten sposób komponent zamykający zostanie usunięty z systemu zamknięć innego klienta. Zostanie utworzone zadanie konserwacyjne.

> Wykonać aktualizację komponentu zamykającego, dla którego anulowano udostępnienie, za pomocą smartfona z uprawnieniem do konserwacji lub opcjonalnej stacji kodującej. Status komponentu zamykającego po zakończonej aktualizacji będzie ponownie aktualny.

Uwaga: Dopiero po aktualizacji komponentu zamykającego nośniki innego klienta nie będą mogły go blokować.

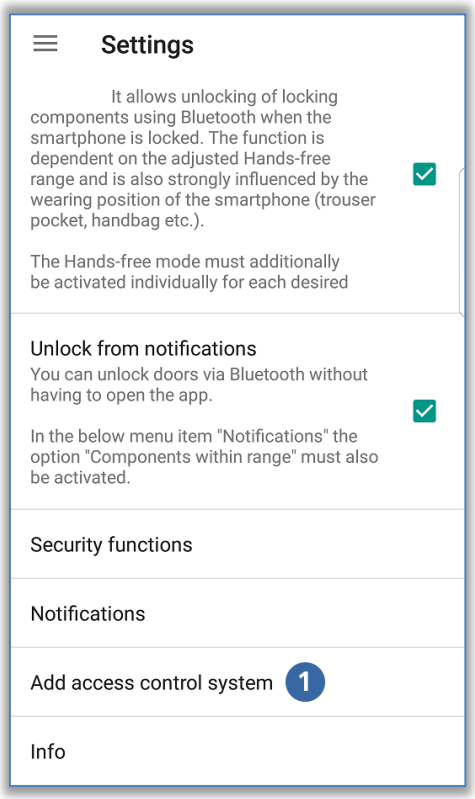
Kasowanie zezwoleń komponentów zamykających jest możliwe jedynie w systemie, z którego zezwolenie zostało udzielone.

Jeśli nie zastosowano kodu zezwolenia i został on usunięty zgodnie ze wskazówkami zawartymi w tym rozdziale, aktualizacja komponentu zamykającego nie będzie konieczna.

10.6 Używanie smartfona w kilku systemach

Istnieje możliwość zarejestrowania smartfona w kilku systemach zamknięć i stosowania jako nośnika.

> W aplikacji AirKey otworzyć menu główne i wybrać opcje ***Ustawienia*** → ***Dodaj system zamknięć*** ❶.



Rys. 298: Dodawanie systemu zamknięć

> W systemie Android automatycznie pojawi się okno dialogowe do wprowadzenia kodu rejestracji. W przypadku systemu iOS należy wybrać opcję ***Już otrzymano kod***

rejestracji, aby pominąć wprowadzanie numeru telefonu i przejść do wprowadzania kodu rejestracji.

> Wprowadzić kod rejestracyjny otrzymany od administratora systemu zamknięć, a następnie stuknąć opcję ***Zarejestruj***.

> Jeśli aktywowałeś kod PIN dla aplikacji AirKey, musisz go wprowadzić i potwierdzić.

Smartfon zostanie zarejestrowany w kolejnym systemie zamknięć AirKey.

Jeśli poprzez wiadomość SMS został wysłany kod rejestracji dla kolejnego systemu zamknięć, wystarczy dotknąć link w SMS-ie, aby automatycznie zainicjować i przeprowadzić rejestrację.

Odpowiednio przesuwając palcem po ekranie smartfona można przełączać pomiędzy widokami uprawnień poszczególnych systemów zamknięć i zbiorczym przeglądem uprawnień.

Firma EVVA zaleca stosowanie kodu PIN. Służy on jako dodatkowy poziom zabezpieczenia i można go w późniejszym okresie aktywować lub dez-aktywować. Bliższe informacje na ten temat można znaleźć w rozdziale Aktywowanie kodu PIN.

11 Interfejs AirKey Cloud (API)

AirKey Cloud Interface to interfejs (API) do łączenia z systemami zewnętrznymi na bazie protokołu REST. Interfejs ten umożliwia sterowanie określonymi funkcjami AirKey z oprogramowania zewnętrznego (np.: system księgujący lub Check-In).

W tym celu oprogramowanie zewnętrzne musi być połączone z modułem zarządzania online AirKey i specjalnie dostosowane, aby mogło wysyłać wymagane polecenia i przetwarzać otrzymywane odpowiedzi.

Zakres dostępnych funkcji i odpowiadające im polecenia znajdziesz w opisie API. Implementację wykona Twój integrator lub programista zastosowanego oprogramowania zewnętrznego.

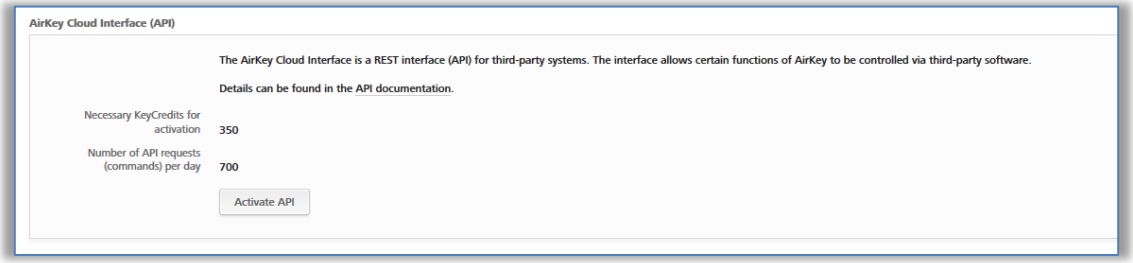
Wypróbuj przykładowo funkcję interfejsu AirKey Cloud przy pomocy aplikacji Demonstracja EVVA AirKey Cloud Interface.

W razie używania interfejsu AirKey Cloud pamiętaj o wystarczająco dużym kredycie. Najlepiej skorzystaj z opcji KeyCredits Unlimited. Gdy kredyt zostanie zużyty lub jest na wyczerpaniu, wszyscy administratorzy systemu zamknięć AirKey są o tym informowani powiadomieniem e-mail. Takie powiadomienie jest wysyłane tylko do tych administratorów, którzy uaktywnili opcję ***Chcę otrzymywać pocztą elektroniczną ważne informacje od firmy EVVA (np. informacje o niskim stanie KeyCredits) (zalecane)***. Takie powiadomienie e mail możesz w każdej chwili indywidualnie edytować dla pojedynczego administratora (patrz rozdział Edycja administratora).

11.1 Uaktywnienie interfejsu AirKey Cloud

Do uaktywnienia interfejsu AirKey Cloud konieczne jest co najmniej 350 jednostek KeyCredit. Do tego celu należy użyć dostępnego kredytu ilościowego jednostek KeyCredit lub odpowiedniej karty do zdrapywania **KeyCredits AirKey Cloud Interface**.

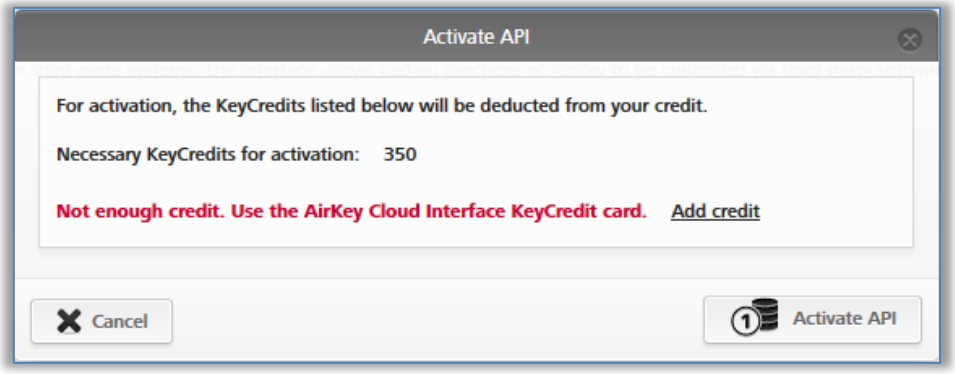
> Kliknij ***Ustawienia*** na zakładce ***Informacje ogólne*** na ***Uaktywnij API***.



Rys. 299: Ogólne ustawienia interfejsu AirKey Cloud (API)

> Jeżeli jest dostępna dostateczna ilość jednostek kredytu, potwierdź dialog ponownie poleceniem ***Uaktywnij API***. Jeżeli kredyt jest niewystarczający, zostanie wyświetlony

komunikat informacyjny. Można wtedy doładować kredyt bezpośrednio korzystając z łącza.



Rys. 300: Uaktywnij API

W ten sposób interfejs AirKey Cloud został uaktywniony. Interfejs AirKey Cloud musi być uaktywniany tylko jednorazowo dla każdego systemu zamknięć, aby można było z niego korzystać.

Po uaktywnieniu otrzymasz informacje o punkcie końcowym (do którego muszą być wysyłane wszystkie polecenia API) oraz o limicie wywołań API (liczba dostępnych wywołań API na dzień). Jako żądanie API liczone jest polecenie, wysyłane przez oprogramowanie zewnętrzne do systemu AirKey.

Limit wywołań API jest resetowany codziennie o godzinie 00:00 UTC. Po przekroczeniu limitu wywołań API informowani są o tym powiadomieniami e-mail wszyscy administratorzy systemu zamknięć AirKey. Takie powiadomienie jest wysyłane tylko do tych administratorów, którzy uaktywnili opcję ***Chcę otrzymywać pocztą elektroniczną ważne informacje od firmy EVVA (np. informacje o niskim stanie KeyCredits) (zalecane)***. Takie powiadomienie e mail możesz w każdej chwili indywidualnie edytować dla pojedynczego administratora (patrz rozdział Edycja administratora).

Jeżeli liczba wywołań API na dzień jest niewystarczająca dla Twojego zastosowania, zwrć się do Wsparcia technicznego EVVA.

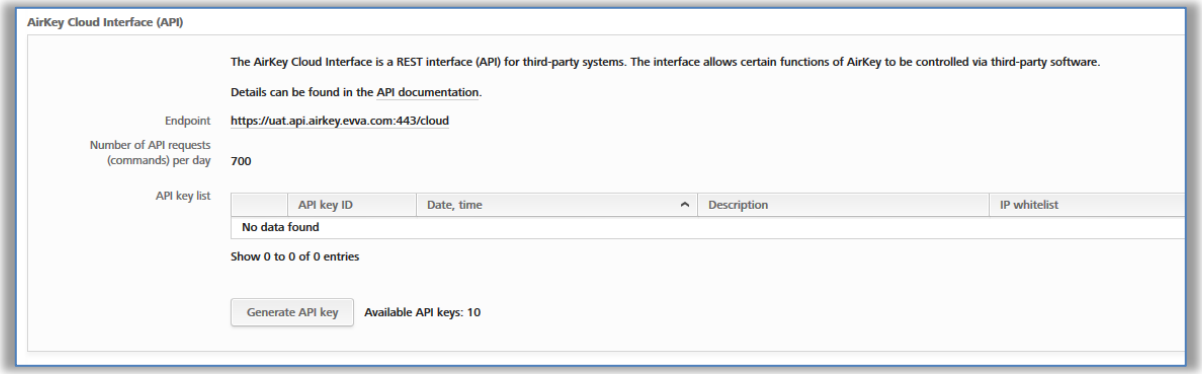
11.2 Generuj klucz API

Komunikacja między systemem AirKey i oprogramowaniem zewnętrznym jest zabezpieczona kluczem API. Tylko osoba znająca klucz API, może wysyłać polecenia przez interfejs AirKey do swojego systemu zamknięć. Każdy system zamknięć z aktywnym interfejsem AirKey Cloud korzysta z własnych kluczy API.

Akcje wykonywane przez interfejs AirKey Cloud, są także protokołowane w protokole systemowym systemu zamknięć AirKey. Jako administrator wykorzystywana jest w tym przypadku pierwsza część klucza API, mianowicie identyfikator klucza API.

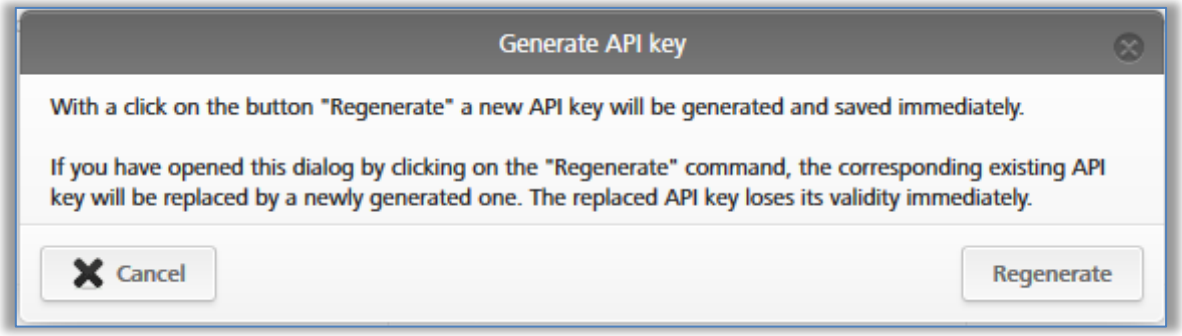
Po uaktywnieniu możesz wygenerować niezbędne do komunikacji klucze API.

> Kliknij w ***Ustawieniach*** na zakładce ***Ogólne informacje*** na polecenie ***Wygeneruj klucz API***.



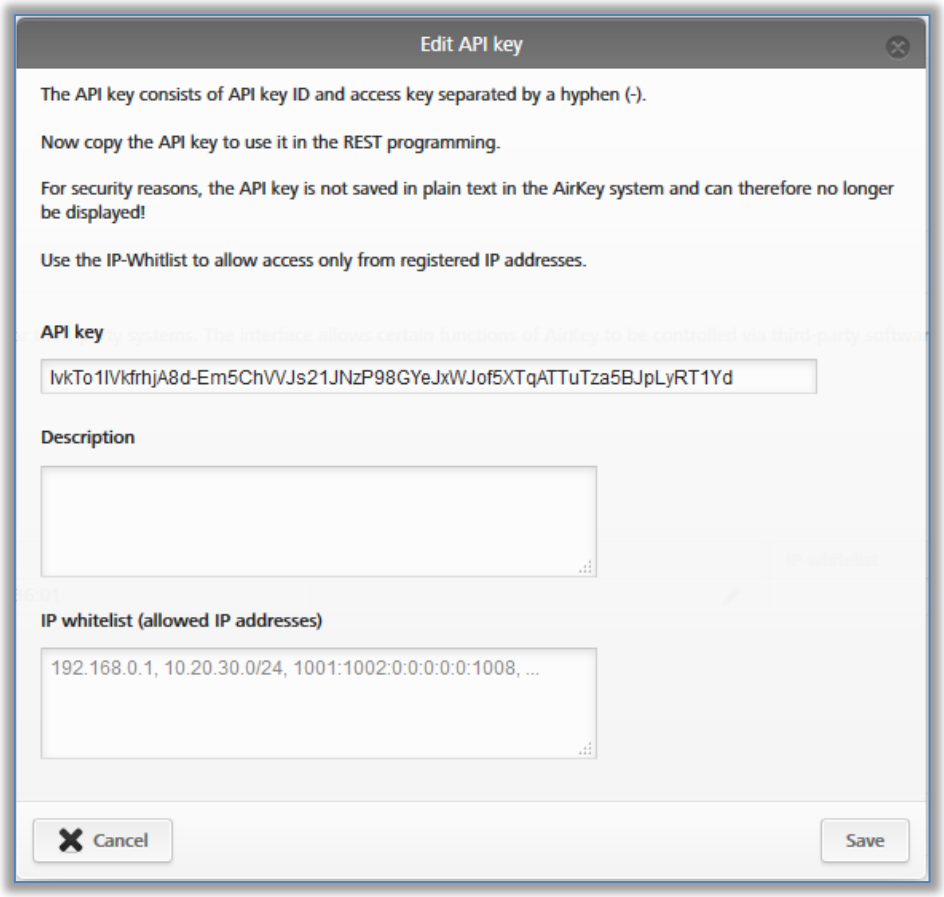
Rys. 301: Wygeneruj klucz API

> Potwierdź dialog ponownie poleceniem ***Wygeneruj klucz API***.



Rys. 302: Dialog generowania klucza API

> Przydziel opis, np. nazwę oprogramowania zewnętrznego i ogranicz opcjonalnie adresy IP uprawnione do wysyłania wywołań API za pomocą IP-Whitelist.



Rys. 303: Szczegóły generowania kluczy API

Skorzystaj z funkcji IP-Whitelist, aby zwiększyć bezpieczeństwo. Do odnośnego klucza API wpisz tylko te adresy IP, które mają prawo wysyłania wywołań API do Twojego systemu zamknięć AirKey.

Na listę IP-Whitelist można wpisywać adresy IP w formacie IPv4 a także IPv6. Jako separator między wieloma adresami zastosuj przecinek (,).

Ze względu na bezpieczeństwo, klucz API jest wyświetlany w całości tylko raz. Zapisz go w bezpiecznym miejscu lub używaj go do swojego oprogramowania zewnętrznego.

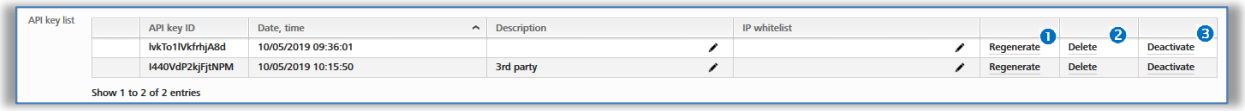
> Wprowadzone dane dotyczące klucza API zapisz, klikając polecenie ***Zapisz***.

Do każdego systemu zamknięć AirKey można wygenerować maksymalnie 10 kluczy API. Umożliwia to sterowanie systemu zamknięć AirKey przez oprogramowanie zewnętrzne.

Wygenerowany klucz API jest listowany w ogólnych ustawieniach, gdzie może być też później edytowany.

11.3 Edytuj klucz API

Opis i IP-Whitelist istniejących kluczy API można później edytować w ***Ustawieniach*** na zakładce ***Ogólne informacje,*** korzystając z symbolu ołówka. Dodatkowo dla poszczególnych kluczy API dostępne są funkcje ***Wygeneruj nowy***, ***Kasuj*** i ***Wyłącz*** lub ***Reaktywuj***.



Rys. 304: Edytuj klucz API

11.3.1 Generuj nowy klucz API

Istniejący klucz API jest przy tym zastępowany przez nowy klucz. Zastąpiony klucz API traci ważność.

> Kliknij ***Ustawienia*** na zakładce ***Ogólne informacje,*** na liście kluczy API, na ***Wygeneruj nowy*** ❶.

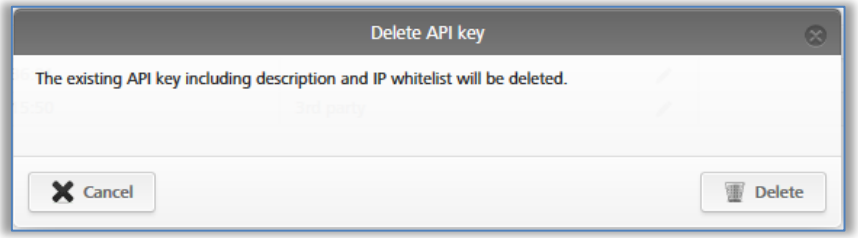
> Wszystkie dalsze operacje są identyczne jak w funkcji Wygeneruj klucz API.

11.3.2 Usuń klucz API

Zostanie skasowany istniejący klucz API. Zostanie on usunięty z listy kluczy API i straci ważność. Skasowanie kluczy API zwiększa odpowiednio liczbę dostępnych kluczy API.

> W ***Ustawieniach*** na zakładce ***Ogólne informacje,*** na liście kluczy API, kliknij na ***Kasuj*** ❷.

> Potwierdź dialog poleceniem ***Kasuj***, aby definitywnie skasować klucz API.



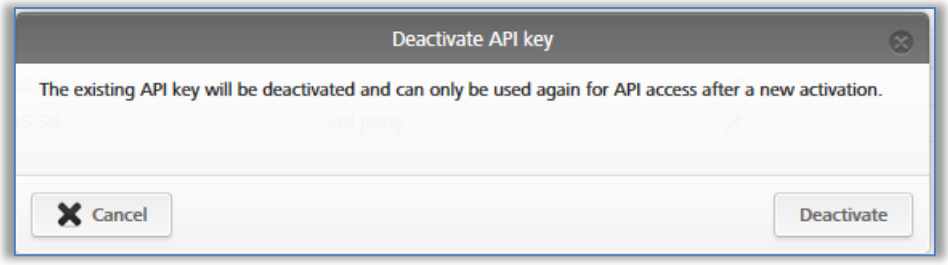
Rys. 305: Kasuj klucz API

11.3.3 Wyłączanie i uaktywnianie klucza API

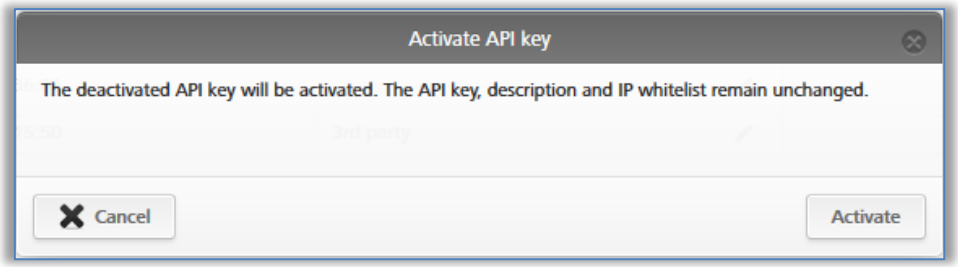
Aktywny klucz API jest wyłączany lub wyłączony klucz API jest ponownie uaktywniany. Wyłączony klucz API jest nieważny i nie może wysyłać wywołań API do systemu zamknięć AirKey. Klucz API oraz jego opis i IP-Whitelist nie zmieniają się wskutek wyłączania i uaktywniania.

> W ***Ustawieniach*** na zakładce ***Ogólne informacje,*** kliknij na liście kluczy API na ***Wyłącz*** ❸ lub ***Uaktywnij***.

> Potwierdź dialog poleceniem ***Wyłącz*** lub ***Uaktywnij***, aby zakończyć procedurę.



Rys. 306: Wyłącz klucz API



Rys. 307: Uaktywnij klucz API

11.4 Interfejs AirKey Cloud – środowisko testowe

Środowisko testowe umożliwia wypróbowanie interfejsu AirKey Cloud (API) przed jego uruchomieniem w środowisku zabezpieczonym z wykorzystaniem danych testowych.

Jego celem jest przede wszystkim wsparcie dla integratorów lub programistów oprogramowania zewnętrznego w ramach integracji z interfejsem AirKey Cloud. Środowisko testowe jest dostępne także przed uaktywnieniem interfejsu AirKey Cloud.

W środowisku testowym nie są pobierane jednostki KeyCredit. Ponadto środowisko testowe nie wysyła wiadomości SMS.

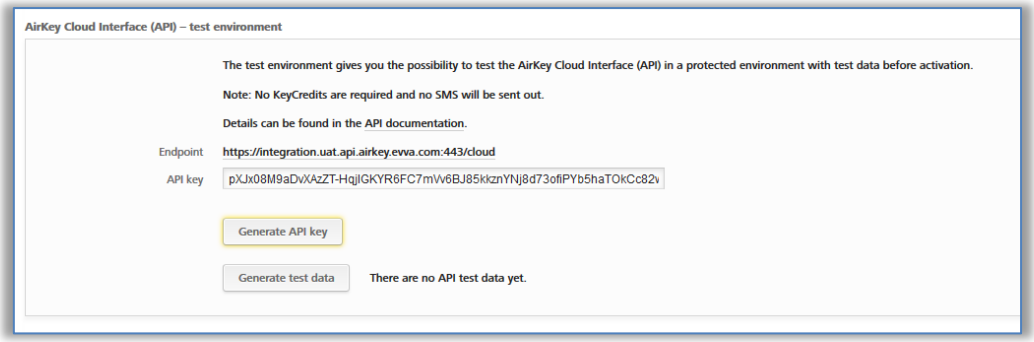
Środowisko testowe interfejsu AirKey Cloud (API) jest dostępne przez własny punkt końcowy (do którego muszą być wysyłane polecenia API).
Punkt końcowy ("Endpoint"): https://integration.api.airkey.evva.com:443/cloud

11.4.1 Generuj dane testowe

Aby skorzystać ze środowiska testowego po raz pierwszy, należy najpierw wygenerować dane testowe.

Wygenerowanie danych testowych wymaga wcześniejszego wygenerowania klucza API.

> W ***Ustawieniach*** na zakładce ***Ogólne informacje*** kliknij ***Generuj dane testowe***.



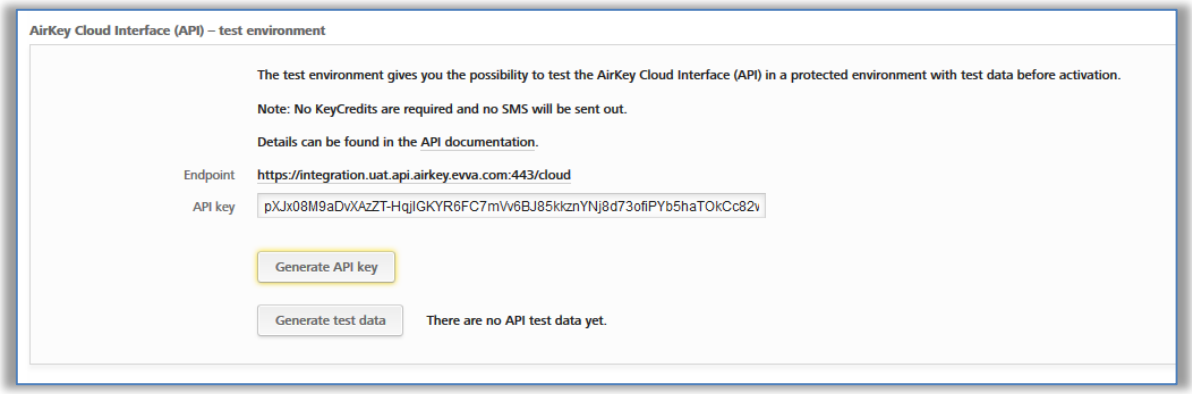
Rys. 308: Generuj dane testowe

Dane testowe zostały wygenerowane. Dane testowe umożliwiają wypróbowanie każdego żądania API z dokumentacji API. Dane testowe muszą być najpierw wygenerowane.

11.4.2 Generuj klucz API

Klucz API jest niezbędny także do komunikacji z interfejsem AirKey Cloud (API) – w środowisku testowym. Bez tego klucza API do środowiska testowego nie mogą być wysyłane żądania API. W porównaniu z prawidłowym interfejsem AirKey Cloud klucz API środowiska testowego jest wysyłany w formacie tekstowym.

> W ***Ustawieniach*** na zakładce ***Ogólne informacje*** w sekcji ***AirKey Cloud Interface (API) – środowisko testowe*** kliknij ***Wygeneruj klucz API***.



Rys. 309: Wygeneruj klucz API w środowisku testowym

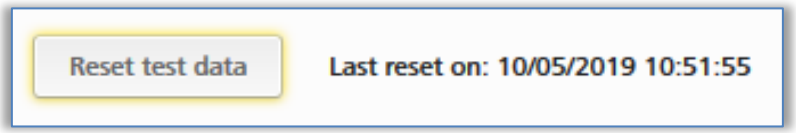
Przez ponowne kliknięcie ***Wygeneruj klucz API*** istniejący klucz API jest zastępowany przez nowy. Zastąpiony klucz API nie może już być wykorzystywany.

Po każdym logowaniu należy od nowa wygenerować klucz API.

11.4.3 Resetuj dane testowe

Dane testowe interfejsu AirKey Cloud – w środowisku testowym można przywrócić jednym kliknięciem do stanu pierwotnego. W ten sposób można wykonać wszystkie testy na tych samych danych testowych.

> W ***Ustawieniach*** na zakładce ***Ogólne informacje*** w sekcji ***Interfejs AirKey Cloud (API) –*** kliknij na ***Resetuj dane testowe.***



Rys. 310: Resetuj dane testowe środowiska testowego

Zresetowanie danych testowych jest potwierdzane komunikatem o udanej operacji. Czas ostatniego resetowania jest wyświetlany w punkcie ***Interfejs AirKey Cloud (API) – środowisko testowe***.

12 Sygnalizacja komponentów zamykających

Komponenty zamykające wskazują zdarzenia za pomocą różnych sygnałów optycznych i akustycznych.

Numer sygnału	Zdarzenie	Optyczny sygnał*)	Akustyczny sygnał*)	Wskazówka
Sygnał 1	Proces odryglowania za pomocą upraw-nionego nośnika	●●●●●	śśśśś	
Sygnał 2	Koniec okresu zezwolenia	●●●●●	nnnnn	
Sygnał 3	Proces odryglowania za pomocą nieuprawnionego nośnika	●●-●●-●●-●●	ww-ww-ww-ww	
Sygnał 7	Ostrzeżenie o rozładowanej baterii (wskazywane w Module zarządzania online systemu AirKey, w tabeli komponentów zamykających i szczegółów danego komponentu zamykającego za pomocą symbol "Bateria rozładowana".)	●●--●●--●●--●●	w----w----w----w	Sygnał jest emito-wany podczas wkładania rozłado-wanych baterii zamiast sygnału 8 i podczas operacji odryglowania przed sygnałem 1. Po pierwszym zasygnalizowaniu możliwe jest wyko-nanie 1000 opera-cji odryglowania lub dwa tygodnie działania w trybie czuwania (w tem-peraturze pokojo-wej i przy zasto-sowaniu karty, breloka do klucza, bransoletki lub klucza Combi).
Sygnał 8	Włożenie nowych baterii lub ponowne uruchomienie komponentu	●●--●●--●●	nn--śś--ww	

Numer sygnału	Zdarzenie	Optyczny sygnał*)	Akustyczny sygnał*)	Wskazówka
Sygnał 9	Nośnik bez segmentacji EVVA; nośnik obcego systemu	●●●	Brak	Nie jest stosowane. Do tego celu używa się wyłącznie sygnału 3.
Sygnał 10	Błąd komunikacji lub sprzętu w komponencie zamykającym	●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●	śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś	Sygnalizacja występuje np. w razie nieprawidłowego połączenia pomiędzy gałką i modułem elektronicznym wkładki.
Sygnał 11	Aktualizacja firmware komponentu zamykającego	●-●-●-●-●… (okres 1 s, impuls 12 ms)	Brak	Czas trwania: aż do zakończenia komunikacji
Sygnał 12	Pomyślna aktualizacja komponentu zamykającego / nośnika	●●-●●	wwwww	
Sygnał 13	Niepomyślna aktualizacja komponentu zamykającego / nośnika	●●-●●	nnnnn	
Sygnał 14	Proces odczytu nośnika AirKey	●-●-●-●-●-●… (okres 100 ms, impuls 10 ms)	Brak	Czas trwania: aż do zakończenia komunikacji
Sygnał 15	Dostępność funkcji Bluetooth i wzbudzenia wkładki AirKey (np. poprzez dotknięcie)	●-●-●-●-●… (okres 1,5 s)	Brak	
Sygnał 16	Rozpoczęcie stałego otwarcia	●●●---●●●	śśś---www	
Sygnał 17	Zakończenie stałego otwarcia	●●●---●●●	www---śśś	
Sygnał 18	Tryb awaryjny baterii wkładki AirKey	●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●● ●●--●●--●●--●●	w----w----w----w śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś w----w----w----w śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś--- śśś---śśś nn--śś--ww w----w----w----w	Przyczyna: Jedna z baterii została włożona nieprawidłowo lub jest rozładowana.

*) Objaśnienia do sygnałów:

Sygnały optyczne: żółty ●, czerwony ●, zielony ●, niebieski ●

Sygnały akustyczne: w = wysoki dźwięk, ś = średni dźwięk, n = niski dźwięk

Każdy sygnał oznacza czas trwania wynoszący 50 ms, pauzy oznaczono znakiem "-".

13 Parametry i limity systemu AirKey

W tym rozdziale opisano maksymalną liczbę konfiguracji nośnika i komponentu zamykającego.

13.1 Moduł zarządzania online systemu AirKey

Liczba możliwych komponentów zamykających, stref, osób i nośników – bez ograniczeń.

13.2 Komponenty zamykające AirKey

- Zapis 1000 ostatnich wpisów do protokołów bez aktualizacji.
- Zarządzanie maks. 1000 wpisów na czarną listę.
- Możliwość maks. 96 przypisań do strefy.
- Możliwość przyznania maks. 250 zezwoleń (udostępnień) do innych klientów.

13.3 Karty, breloki do kluczy, bransoletka lub klucze Combi

- Zapis maks. 256 wpisów do protokołów bez aktualizacji.
- Możliwość przypisania maks. 150 uprawnień do poszczególnych drzwi.
- Możliwość przypisania maks. 100 uprawnień do stref (przypisanie 12 indywidualnych uprawnień, każde z 8 możliwymi dostępami, zatem łącznie można przypisać tylko 96 uprawnień do stref).

13.4 Aplikacja AirKey

- Zapis maks. 256 wpisów do protokołów bez aktualizacji.
- Nieograniczone liczba uprawnień do poszczególnych drzwi i stref.

14 Kiedy następuje pobranie (wyksięgowanie) jednostek KeyCredit?

Do bieżącej eksploatacji systemu zamknięć niezbędne są jednostki KeyCredit, służące do przekazywania lub zmiany uprawnień dostępu.

Jednostki KeyCredit są wyksięgowywane tylko w przypadku kredytu ilościowego. Jeśli dostępny jest ważny kredyt czasowy, system korzysta z kredytu czasowego a kredyt ilościowy zostaje nienaruszony.

Pobranie (wyksięgowanie) jednostek KeyCredit następuje w przypadku następujących operacji:

- Przydzielanie nowych uprawnień i ich potwierdzanie
- Zmiana istniejących uprawnień i ich potwierdzanie
- Reaktywowanie dezaktywowanych nośników, o ile zostaną zachowane uprawnienia dezaktywowanego nośnika
- Przy uaktywnianiu interfejsu AirKey Cloud (API)

W przypadku nowych uprawnień lub zmiany uprawnień jednostki KeyCredit są pobierane dopiero wówczas, gdy następuje przygotowanie nośnika. Jedno przygotowanie kosztuje jedną jednostkę KeyCredit. Można jednocześnie utworzyć lub zmienić kilka uprawnień – zostanie wówczas pobrany tylko jeden KeyCredit.

W przypadku kasowania uprawnień, dezaktywacji lub wyczyszczenia nośników jednostki KeyCredit nie są pobierane.

15 Usuwanie błędów

System AirKey to elektroniczny system zamknięć, który został wszechstronnie przetestowany i sprawdzony. Jeśli mimo to wystąpią usterki lub problemy, w tym rozdziale można znaleźć porady i wskazówki umożliwiające ich usunięcie.

15.1 Komunikacja w ramach systemu jest niemożliwa

Jeśli zarejestrowanie smartfona lub aktualizacja komponentu zamykającego AirKey nie jest możliwa, należy wykonać poniższe czynności sprawdzające:

- Sprawdzić, czy smartfon ma połączenie z Internetem (WLAN lub mobilny transfer danych) i w razie potrzeby aktywować je.
- Sprawdzić, czy port 443 w infrastrukturze IT jest zablokowany. Te porty są potrzebne do komunikacji w ramach systemu AirKey i muszą być dostępne. patrz rozdział Wymagania systemowe.

15.2 Komponent zamykający rzadko lub wcale nie rozpoznaje nośników

Jeśli przy pewnym komponencie zamykającym nośniki są rozpoznawane rzadko lub wcale (w porównaniu do innych komponentów zamykających), należy wykonać poniższe czynności sprawdzające:

- Pamiętać o tym, aby nośnik podczas identyfikacji był trzymany nieruchomo przy czytniku i odczekać, aż pojawi się sygnalizacja kolorem zielonym komponentu zamykającego. (Sygnalizacja kolorem niebieskim oznacza tylko komunikację między smartfonem a komponentem zamykającym.)
- Jeśli komponent zamykający nie reaguje, sprawdzić prawidłowe położenie nośnika. Na przykład klucz Combi należy zbliżyć z tej strony, na której znajduje się symbol RFID.
- Jeśli nie przyniesie to oczekiwanych rezultatów, należy odczekać 50 sekund bez przeprowadzania identyfikacji na czytniku, aby komponent zamykający na nowo skalibrował pole elektryczne czytnika. Przytrzymanie metalowego przedmiotu przy module czytnika spowoduje ręczną rekalibrację.

15.3 Nośniki nie są rozpoznawane

Jeśli określony nośnik nie zostaje rozpoznawany przez komponenty zamykające, należy wykonać następujące czynności sprawdzające:

- Jeśli chodzi o smartfon, należy sprawdzić, czy funkcja NFC lub Bluetooth została aktywowana Ewentualnie należy ponownie uruchomić połączenie NFC lub Bluetooth, zwracając uwagę na prawidłowe położenie smartfona względem modułu czytnika, Należy pamiętać, że mogą wystąpić różnice w zależności od typu smartfona.
- Jeśli moduł czytnika komponentu zamykającego lub stacji kodującej w ogólnie nie reaguje na nośnik, należy przytrzymać nośnik przez około 10 sekund przy czytniku

komponentu zamykającego lub stacji kodującej. Nośnik powinie samodzielnie dokonać naprawy. Zakończenie operacji można stwierdzić, gdy komponent zamykający lub stacja kodująca zacznie sygnalizować w normalny sposób.

15.4 Odśrubowanie gałki wkładki AirKey jest niemożliwe

Jeśli odśrubowanie gałki wkładki AirKey nie będzie możliwe, należy wykonać poniższe czynności:

- Upewnić się, że podczas demontażu gałki zastosowano narzędzie montażowe do wkładki AirKey.
- Wkładki AirKey w europrofilu mają na stronie czołowej modułu elektronicznego otwór serwisowy, poprzez który można zamocować trzpień gałki za pomocą pasującego sztyftu metalowego. Zalecamy tutaj użycie zestawu narzędzia montażowego nr 2.

Procedura:

- Wprowadzić sztyft metalowy z narzędzia montażowego nr 2 w otwór serwisowy od strony czołowej wkładki w europrofilu.
- Obracać gałkę wokół własnej osi tak długo, aż będzie można wsunąć sztyft metalowy zauważalnie głębiej w otwór serwisowy. Przytrzymać sztyft metalowy w tej pozycji i zdemontować gałkę za pomocą narzędzia montażowego.
- Wyjąć sztyft metalowy po demontażu gałki.
- Jeśli użytkownik nie dysponuje wkładką AirKey w europrofilu lub zamontowana została wkładka AirKey w okuciu lub rozecie z zabezpieczeniem przed wyciągnięciem rdzenia, należy przytrzymać uprawniony nośnik przy module czytnika, aby nastąpiło zasprzęglenie wkładki. W trakcie czasu odblokowania (gdy wkładka jest zasprzęglona) należy osadzić narzędzie montażowe. W tym przypadku wkładka nie wysprzęgli się i można ją łatwo odkręcić.

15.5 Komponent zamykający sygnalizuje błąd sprzętowy

Gdy komponent zamykający AirKey zgłasza błąd sprzętowy (patrz Sygnalizacja komponentów zamykających), istnieje możliwość, że gałka / moduł czytnika nie zostały połączone z przynależnym modułem elektronicznym / przynależną centralką sterującą.

Sprawdzić styki, wtyczki i połączenia zgodnie z instrukcją montażu.

15.5.1 Wkładka AirKey

- Upewnić się, że pierścień uszczelniający na trzpieniu wkładki został prawidłowo osadzony i ponownie umieścić gałkę nad wkładką, obracając zgodnie z ruchem wskazówek zegara, aż do wyczuwalnego oporu.
- Zdjąć narzędzie montażowe.
- Obrócić gałkę w kierunku przeciwnym do ruchu wskazówek zegara, aż się wyczuwalnie zatrzaśnie.
- Upewnić się, że gałka i moduł elektroniczny zostały prawidłowo zatrzaśnięte.

15.5.2 Czytnik naścienny AirKey

> Zadbać o to, aby moduł czytnika i centralka sterująca AirKey zostały prawidłowo połączone. Ewentualnie sprawdzić okablowanie i połączenia wtykowe.

15.6 Elektroniczna gałka działa z trudnością

W zależności od wystającej długości wkładki z rozety wkładki lub okucia, wkładka ewentualnie może działać z trudnością z uwagi na tarcie uszczelki pomiędzy korpusem wkładki i gałką elektroniczną. W takim przypadku istnieje możliwość wyjęcia uszczelki w obszarach wewnętrznych.

Jeśli jednak zajdzie potrzeba skorzystania ze wsparcia, należy zwrócić się do partnera firmy EVVA (Wsparcia technicznego EVVA).

16 Ważne wskazówki

16.1 System

Należy zwrócić szczególną uwagę na fakt, że istniejący system AirKey może podlegać przepisom ustawowym, zwłaszcza w zakresie obowiązków rejestracji/uzyskania zezwoleń wynikających z ustawy o ochronie danych. Stosownie do tego obowiązku firma EVVA Sicherheitstechnologie GmbH nie przejmuje żadnej odpowiedzialności i gwarancji w zakresie eksploatacji zgodnej z prawem.

Do komunikacji w systemie AirKey stosuje się porty internetowe 443 i 7070. Należy pamiętać, aby te porty nie były zablokowane. W przypadku zastosowania mobilnej sieci danych za zarządzanie portem odpowiada operator sieci komórkowej. Jeśli wystąpią problemy podczas stosowania mobilnej sieci danych w systemie AirKey, należy skontaktować się ze swoim operatorem sieci komórkowej.

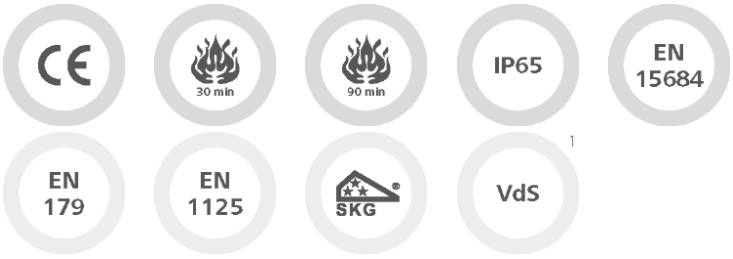
Uprawnienia należy tworzyć przy zapewnieniu możliwie krótkiego czasu obowiązywania, aby zapewnić wysoki poziom bezpieczeństwa systemu i w razie utraty nośnika nie rozszerzać nadmiernie liczby wpisów do czarnej listy. Nośniki z nieograniczonymi uprawnieniami bez daty upływu ważności należy przygotowywać tylko jako nośniki awaryjne (np. klucz dla straży pożarnej).

Należy zawsze pracować z aktualną konfiguracją całego systemu, aby zapewnić wysoki poziom rozwiązania. Wskazówki bezpieczeństwa dotyczące poszczególnych systemów można znaleźć, korzystając z poniższych linków:

Wkładka, kłódka: PDF

Czytnik naścienny, centralka sterująca: PDF

Normy i wytyczne

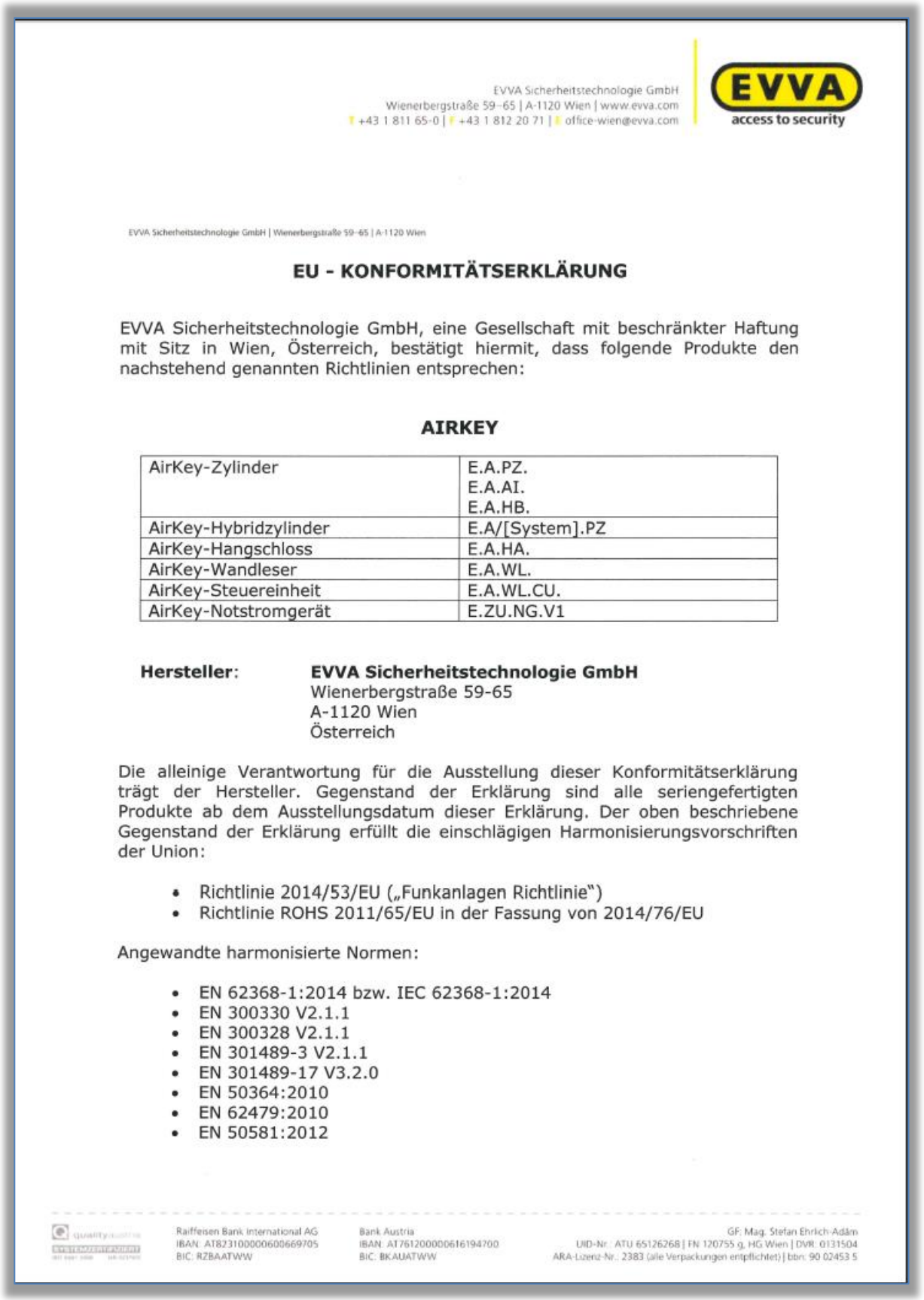


Spełnia dyrektywy CE | EN 1634: 30 minut | EN 1634: 90 minut | stopień ochrony IP65 | EN 15684 | odpowiednie do zamków wg normy EN 179/1125 (w przypadku użycia funkcji antypanicznej FAP)

SKG | VdS[1]

[1] W przygotowaniu

17 Deklaracja zgodności



EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA
access to security

EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59–65 | A-1120 Wien

EU - KONFORMITÄTSERKLÄRUNG

EVVA Sicherheitstechnologie GmbH, eine Gesellschaft mit beschränkter Haftung mit Sitz in Wien, Österreich, bestätigt hiermit, dass folgende Produkte den nachstehend genannten Richtlinien entsprechen:

AIRKEY

AirKey-Zylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridzylinder	E.A/[System].PZ
AirKey-Hangschloss	E.A.HA.
AirKey-Wandleser	E.A.WL.
AirKey-Steuereinheit	E.A.WL.CU.
AirKey-Notstromgerät	E.ZU.NG.V1

Hersteller: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Wien
Österreich

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt der Hersteller. Gegenstand der Erklärung sind alle seriengefertigten Produkte ab dem Ausstellungsdatum dieser Erklärung. Der oben beschriebene Gegenstand der Erklärung erfüllt die einschlägigen Harmonisierungsvorschriften der Union:

- Richtlinie 2014/53/EU („Funkanlagen Richtlinie")
- Richtlinie ROHS 2011/65/EU in der Fassung von 2014/76/EU

Angewandte harmonisierte Normen:

- EN 62368-1:2014 bzw. IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

Raiffeisen Bank International AG
IBAN: AT823100000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT761200000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5

Notifizierte Stelle:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Wien
Kennnummer: 0408

Die Komponenten werden mit einer Firmware ausgeliefert, die den bestimmungsgemäßen Betrieb der Funkanlage ermöglichen.

Unterzeichnet für und im Namen von EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Geschäftsführer

Wien, 13.06.2017

EU-Konformitätserklärung_AIRKEY / 2

18 Declaration of Conformity

EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA
access to security

EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59–65 | A-1120 Wien

EU – DECLARATION OF CONFORMITY

EVVA Sicherheitstechnologie GmbH, a limited liability company having its seat in Vienna, Austria, herewith confirms compliance of the following products with the directives below:

AIRKEY

AirKey-Cylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridcylinder	E.A/[System].PZ
AirKey-Padlock	E.A.HA.
AirKey-Wallreader	E.A.WL.
AirKey-Control Unit	E.A.WL.CU.
AirKey-Emergency Power Device	E.ZU.NG.V1

Manufacturer: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Vienna
Austria

This declaration of conformity is issued under the sole responsibility of the manufacturer. Object of this declaration are all serial manufactured products since the issue date of this declaration. The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

- Directive 2014/53/EU („Directive for radio equipment devices")
- Directive ROHS 2011/65/EU in the version of 2014/76/EU

Relevant harmonised Standards:

- EN 62368-1:2014 respectively IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

Notified body:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Vienna
Number: 0408

The components are delivered with a firmware which allows the radio equipment to operate as intended.

Signed for and on behalf of EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Managing Director

Vienna, 13.06.2017

EU-Declaration of Conformity_AIRKEY / 2

19 Spis rysunków

20 Glosariusz

W ramach systemu AirKey zastosowano m.in. poniższe pojęcia:

Nazwa	Funkcja
Klient	Właściciel systemu zamknięć, któremu przypisano jednoznaczny numer klienta.
Administrator	Jest to rola użytkownika systemu AirKey, który jest uprawniony do wykonywania wszystkich czynności administracyjnych w Module zarządzanie online systemu AirKey. Dla jednego klienta można utworzyć kilku administratorów. Dla każdego systemu zamknięć AirKey należy utworzyć przynajmniej jednego administratora.
Osoba	Użytkownicy używający nośników. Osobom przypisuje się nośniki z uprawnieniami dostępu dla określonych stref i komponentów zamykających.
Nośniki	Smartfony lub nośniki dostępu, które można dodać do systemów zamknięć AirKey w celu uzyskania dostępu do komponentów zamykających AirKey.
Nośniki dostępu	Są to nośniki NFC pasywne (bez własnego zasilania), które mogą być stosowane w smartfonach i w systemach zamknięć AirKey jako nośniki dostępowe. Obejmują one: karty, przywieszki do kluczy, klucze Combi, bransoletki itd.
Komponenty zamykające	Są to wkładki AirKey (o różnych formach konstrukcyjnych), kłódki i czytniki naścienne AirKey, które mogą otwierać i zamykać drzwi systemu zamknięć.
Zakres	Jest to moduł administracyjny w systemie zarządzania online AirKey, obejmujący szereg komponentów zamykających. Sekcje ułatwiają zarządzanie systemem zamknięć AirKey i nadawanie uprawnień komponentom zamykających.
KeyCredits	Opisuje kredyt w ramach systemu zamknięć AirKey. Kredyt jest potrzebny do przydzielania nowych uprawnień, modyfikowania istniejących uprawnień lub do uaktywniania dodatkowych funkcji AirKey.
Interfejs AirKey Cloud	AirKey Cloud Interface to interfejs (API) do łączenia z systemami zewnętrznymi na bazie protokołu REST. Interfejs umożliwia sterowanie określonymi funkcjami AirKey za pośrednictwem oprogramowania zewnętrznego.
Send a Key	Opisuje jedną z funkcji Modułu zarządzania online systemu AirKey.

	Funkcją ta administrator może szybko tworzyć nowe smartfony i przydzielać uprawnienia albo edytować istniejące uprawnienia smartfonów. Użytkownik smartfona otrzymuje wiadomość SMS, za pomocą której smartfon jest automatycznie rejestrowany w systemie AirKey.
Uwierzytelnienie dwuetapowe	Uwierzytelnienie dwuetapowe, czyli 2FA, stanowi dodatkowy poziom zabezpieczenia przy logowaniu do Modułu zarządzania online systemu AirKey. Oprócz identyfikatora użytkownika i hasła przy logowaniu w drugim etapie sprawdzany jest dodatkowy kod SMS.
Oprogramowanie firmware	Oprogramowanie pracujące na komponentach zamykających, umożliwiające wykonywanie przez nie funkcji AirKey. Oprogramowanie firmware komponentów zamykających może być uaktualniane przez uaktualnienia firmware.
Keyring	W systemie AirKey "Keyring" jest nazwą programu, który służy do zarządzania wszelkimi danymi istotnymi dla systemu AirKey, zapisanymi na pasywnych nośnikach dostępu, takich jak karty, breloki do kluczy, klucze Combi i bransoletki. Gdy dostępna jest nowa wersja programu Keyring w systemie AirKey, nośniki można zaktualizować za pomocą smartfona z uprawnieniem do konserwacji lub za pomocą stacji kodującej.
Zadania konserwacyjne	Są wyświetlane w Module zarządzania online systemu AirKey dla nieaktualnych komponentów zamykających. Dopiero po wykonaniu wszystkich zadań konserwacyjnych systemu zamknięć AirKey system jest aktualny i bezpieczny.
Uprawnienie do konserwacji	Tylko wówczas, gdy smartfon posiada uprawnienie konserwacyjne, można za pomocą takiego smartfona dodawać lub usuwać komponenty (nośniki i komponenty zamykające) z systemu zamknięć. Za pomocą smartfona z uprawnieniem do konserwacji technik konserwacyjny systemu AirKey może również obsługiwać komponenty zamykające będące w stanie fabrycznym. Uprawnienie konserwacyjne należy najpierw aktywować w Module zarządzania online systemu AirKey dla żądanego smartfona.

21 Nota prawna

Wydanie 6, czerwiec 2022

W momencie publikacji nowego podręcznika systemu niniejsze wydanie przestaje obowiązywać. Aktualną wersję podręcznika systemu można pobrać z firmowej strony internetowej: https://www.evva.com/pl/airkey/systemmanual/.

Jest możliwe, że niniejszy podręcznik wykazuje braki lub błędy w druku. Jednak informacje zawarte w tym podręczniku systemu są regularnie sprawdzane a treść poddawana jest korekcie. W przypadku błędów natury technicznej lub błędów drukarskich nie bierzemy odpowiedzialności za ich skutki.

Zmiany w rozumieniu postępu technicznego mogą być wdrażane bez wcześniejszego powiadomienia.

Nota prawna

Wydawca
EVVA Sicherheitstechnologie GmbH

Odpowiedzialność za treść
EVVA Sicherheitstechnologie GmbH

Treść techniczna
Florian Diener, Johannes Ullmann

Doradcy techniczni
Raphael Fasching, Iulian Stanciulescu, Martin Bauer