# 4. Wymagania funkcjonalne

## Zarządzanie kontami użytkowników

4.1.1 Opis i priorytet

*Ta funkcja obejmuje rejestrację, weryfikację, przechowywanie i zarządzanie kontami użytkowników za pomocą Strony Internetowej oraz Interfejsu API. Wysoki priorytet.*

4.1.2 Sekwencje / Odpowiedzi

*Użytkownik rejestruje konto na Stronie Internetowej lub za pośrednictwem API. System weryfikuje dane uwierzytelniające użytkownika i wysyła wiadomość potwierdzającą. Użytkownik loguje się, używając zarejestrowanych danych uwierzytelniających. System pobiera i wyświetla informacje o koncie użytkownika.*

4.1.3 Wymagania funkcjonalne

*REQ-1: System musi zapewnić interfejs rejestracji na Stronie Internetowej i API.*

*REQ-2: Informacje o koncie użytkownika, w tym dane uwierzytelniające, muszą być przechowywane w sposób bezpieczny.*

*REQ-3: Administratorzy muszą mieć możliwość zarządzania kontami użytkowników, w tym aktywacją, dezaktywacją i modyfikacją.*

*REQ-4: System musi dostarczać komunikaty o błędach dla nieprawidłowych danych podczas procesów rejestracji i logowania.*

## Powiadomienia i potwierdzenia poprzez e-mail

4.2.1 Opis i priorytet

*Ta funkcja obejmuje możliwość informowania użytkowników o zmianach, konserwacjach lub wszelkich innych istotnych informacjach poprzez wysyłanie powiadomień e-mailowych. Ponadto, system musi umożliwiać potwierdzenie tożsamości użytkownika za pomocą e-maila. Wysoki priorytet.*

4.2.2 Sekwencje / Odpowiedzi

*System wysyła powiadomienie e-mailowe do użytkowników, zawierające odpowiednie informacje. Użytkownik otrzymuje powiadomienie e-mailowe i może go przeczytać. System umożliwia potwierdzenie tożsamości użytkownika poprzez wysłanie wiadomości e-mailowej z linkiem aktywacyjnym lub kodem weryfikacyjnym.*

4.2.3 Wymagania funkcjonalne

*REQ-5: Użytkownicy powinni mieć możliwość potwierdzenia swojej tożsamości poprzez kliknięcie w link aktywacyjny otrzymanego w e-mailu.*

*REQ-6: System musi obsługiwać wysyłanie e-maili w sposób niezawodny i zabezpieczony.*

*REQ-7: System powinien mieć mechanizmy potwierdzania tożsamości użytkownika poprzez e-mail, na przykład poprzez link aktywacyjny.*

## Zarządzanie użytkownikami I punktami dostępu

4.3.1 Opis i priorytet

*Ta funkcja polega na umożliwieniu administratorom organizacji i operatorom projektów zarządzania kontami użytkowników, przeglądania ich dziennika aktywności oraz zarządzania punktami wejścia/punktami końcowymi poprzez interfejs witryny internetowej. Wysoki priorytet.*

4.3.2 Sekwencje / Odpowiedzi

*Administrator lub operator loguje się do interfejsu witryny internetowej. System prezentuje panel administracyjny z dostępem do funkcji zarządzania użytkownikami i punktami dostępu. Administrator lub operator wybiera odpowiednią opcję, np. zarządzanie kontami użytkowników. System wyświetla listę użytkowników lub punktów dostępu do zarządzania. Administrator lub operator wykonuje odpowiednie działania, takie jak dodawanie, usuwanie, aktywowanie, dezaktywowanie użytkowników lub punktów dostępu. System zapisuje dokonane zmiany i aktualizuje dane użytkowników lub punktów dostępu.*

4.3.3 Wymagania funkcjonalne

*REQ-8: System musi dostarczać interfejs witryny internetowej umożliwiający logowanie administratorom organizacji i operatorom projektów.*

*REQ-9: Interfejs witryny internetowej powinien zawierać panel administracyjny z funkcjonalnościami zarządzania użytkownikami i punktami dostępu.*

*REQ-10: System musi umożliwiać dodawanie, usuwanie, aktywowanie, dezaktywowanie użytkowników i punktów dostępu.*

*REQ-11: Interfejs użytkownika powinien być intuicyjny i łatwy w obsłudze.*

## Zarządzanie użytkownikami i punktami dostępu

4.4.1 Opis i priorytet

*Ta funkcja umożliwia administratorom organizacji i operatorom projektów dostęp do bieżącego stanu systemu i potencjalnych naruszeń bezpieczeństwa. Wysoki priorytet.*

4.4.2 Sekwencje / Odpowiedzi

*Administrator organizacji lub operator projektu loguje się do interfejsu internetowego.System zapewnia status systemu w czasie rzeczywistym i ostrzega o wszelkich naruszeniach bezpieczeństwa. Administrator organizacji lub operator projektu sprawdza stan systemu i w razie potrzeby podejmuje odpowiednie działania. System aktualizuje informacje o stanie w czasie rzeczywistym w miarę zmian sytuacji.*

4.4.3 Wymagania funkcjonalne

*REQ-12: System musi zapewniać bezpieczny interfejs strony internetowej dla administratorów organizacji i operatorów projektów w celu uzyskania dostępu do statusu systemu.*

*REQ-13: Interfejs strony internetowej musi wyświetlać status systemu w czasie rzeczywistym, w tym wszelkie alerty dotyczące naruszenia bezpieczeństwa.*

*REQ-14: System musi umożliwiać administratorom i operatorom podejmowanie działań w oparciu o dostarczone informacje o statusie.*

*REQ-15: System musi dynamicznie aktualizować informacje o stanie i powiadamiać użytkowników o istotnych zmianach.*

## Obsługa danych punktu wejścia i informacje zwrotne o stanie użytkownika

4.5.1 Opis i priorytet

*Ta funkcja zapewnia, że bezpieczny komponent sprzętowy produktu może odbierać dane ze smartfonów za pośrednictwem NFC w punktach wejścia i dostarczać użytkownikom informacje o bieżącym stanie za pośrednictwem ekranu lub innych deterministycznych i intuicyjnych środków. Wysoki priorytet.*

4.5.2 Sekwencje / Odpowiedzi

*Użytkownik zbliża się do punktu wejścia ze smartfonem, aby przesłać dane przez NFC. System odbiera dane ze smartfona i przetwarza żądanie dostępu. System zapewnia użytkownikowi aktualizację statusu żądania dostępu za pośrednictwem ekranu lub innego intuicyjnego mechanizmu informacji zwrotnej. Użytkownik interpretuje informacje zwrotne i podejmuje odpowiednie działania.*

4.5.3 Wymagania funkcjonalne

*REQ-16: Produkt musi być w stanie odbierać dane ze smartfonów za pośrednictwem NFC w punktach wejścia.*

*REQ-17: System musi przetwarzać otrzymane dane i dostarczać użytkownikowi aktualizację statusu.*

*REQ-18: System musi wyświetlać aktualizację statusu w deterministyczny i intuicyjny sposób, na przykład za pomocą ekranu lub innego mechanizmu sprzężenia zwrotnego.*

*REQ-19: System musi rejestrować wszystkie aktualizacje statusu transferu danych i żądań dostępu do celów audytu.*

## Obsługa aktualizacji oprogramowania OTA (Over-the-Air)

4.6.1 Opis i priorytet

*Ta funkcja zapewnia, że produkt może prawidłowo obsługiwać aktualizacje oprogramowania OTA, zachowując funkcjonalność i bezpieczeństwo systemu. Wysoki priorytet.*

4.6.2 Sekwencje / Odpowiedzi

*System otrzymuje powiadomienie o aktualizacji oprogramowania OTA. System planuje aktualizację dla okna konserwacji lub monituje użytkownika o instalację. System pobiera i instaluje aktualizację, zapewniając minimalne zakłócenia w bieżącej pracy. System weryfikuje pomyślną instalację aktualizacji i wznawia normalne działanie.*

4.6.3 Wymagania funkcjonalne

*REQ-20: Produkt musi być w stanie odbierać i przetwarzać powiadomienia o aktualizacjach oprogramowania OTA.*

*REQ-21: System musi planować aktualizacje podczas okien konserwacyjnych lub monitować użytkowników o instalację w odpowiednim czasie.*

*REQ-22: System musi pobierać i instalować aktualizacje w bezpieczny i niezawodny sposób.*

*REQ-23: System musi weryfikować pomyślną instalację aktualizacji i przekazywać informacje zwrotne użytkownikom lub administratorom.*

## Bezpieczne uwierzytelnianie użytkowników i kontrola dostępu

4.7.1 Opis i priorytet

*Ta funkcja zapewnia ochronę produktu przed nieautoryzowanym dostępem poprzez wdrożenie mechanizmów silnego uwierzytelniania i kontroli dostępu. Wysoki priorytet.*

4.7.2 Sekwencje / Odpowiedzi

*Użytkownik próbuje uzyskać dostęp do produktu za pomocą smartfona. System inicjuje proces uwierzytelniania, prosząc o podanie danych uwierzytelniających. Użytkownik podaje prawidłowe dane uwierzytelniające za pośrednictwem aplikacji mobilnej. System weryfikuje dane uwierzytelniające z serwerem kontrolującym i przyznaje dostęp, jeśli został uwierzytelniony.*

4.7.3 Wymagania funkcjonalne

*REQ-24: Produkt musi inicjować żądanie uwierzytelnienia po zbliżeniu smartfona do NFC.*

*REQ-25: Aplikacja mobilna musi bezpiecznie przesyłać dane uwierzytelniające użytkownika do serwera kontrolującego w celu weryfikacji.*

*REQ-26: Serwer kontrolujący musi zweryfikować dane uwierzytelniające użytkownika i odpowiedzieć przyznaniem lub odmową dostępu.*

*REQ-27: Produkt musi odmówić dostępu, jeśli serwer kontrolujący odpowie odmownie.*

*REQ-28: System musi rejestrować wszystkie próby uwierzytelnienia, w tym próby udane i nieudane, do celów audytu.*

## Ograniczenie dostępu dla dwóch urządzeń

4.8.1 Opis i priorytet

*Ta funkcja wymusza zasady, które uniemożliwiają użytkownikom dostęp do produktu za pomocą dwóch różnych smartfonów jednocześnie bez wyraźnego pozwolenia, zwiększając bezpieczeństwo systemu. Wysoki priorytet.*

4.8.2 Sekwencje / Odpowiedzi

*Użytkownik próbuje uzyskać dostęp do produktu za pomocą drugiego smartfona, będąc już zalogowanym na innym urządzeniu. System wykrywa próbę dostępu z dwóch urządzeń i prosi użytkownika o autoryzację. Użytkownik prosi użytkownika uprzywilejowanego o autoryzację do korzystania z drugiego urządzenia. System powiadamia użytkownika uprzywilejowanego o żądaniu autoryzacji. Uprzywilejowany użytkownik udziela lub odrzuca żądanie autoryzacji. System wymusza decyzję użytkownika uprzywilejowanego, zezwalając lub odmawiając dostępu z drugiego urządzenia.*

4.8.3 Wymagania funkcjonalne

*REQ-29: System musi wykrywać jednoczesne próby dostępu z dwóch różnych urządzeń powiązanych z tym samym kontem użytkownika.*

*REQ-30: System musi zapewnić powiadomienie i zażądać autoryzacji od uprzywilejowanego użytkownika, gdy próbowany jest dostęp z dwóch urządzeń.*

*REQ-31: Interfejs użytkownika uprzywilejowanego musi zawierać funkcję zarządzania i odpowiadania na żądania autoryzacji dostępu do dwóch urządzeń.*

*REQ-32: System musi rejestrować wszystkie próby dostępu do dwóch urządzeń i decyzje użytkownika uprzywilejowanego do celów audytu.*

## Organizacja i zarządzanie administratorami

4.9.1 Opis i priorytet

*Ta funkcja umożliwia operatorom projektów tworzenie nowych organizacji i przypisywanie administratorów, którzy mogą zarządzać użytkownikami i prawami dostępu w ramach odpowiednich organizacji. Wysoki priorytet.*

4.9.2 Sekwencje / Odpowiedzi

*Operator projektu inicjuje utworzenie nowej organizacji. System zapewnia operatorowi projektu interfejs do wprowadzania szczegółów organizacji i wyboru administratora. Operator projektu potwierdza utworzenie nowej organizacji i przypisanie administratora. System tworzy nową organizację i przyznaje uprawnienia administratora wybranemu użytkownikowi.*

4.9.3 Wymagania funkcjonalne

*REQ-33: System musi zapewniać interfejs użytkownika dla operatorów projektów w celu tworzenia nowych organizacji.*

*REQ-34: System musi umożliwiać operatorom projektów przypisywanie administratorów do zarządzania użytkownikami i prawami dostępu każdej organizacji.*

*REQ-35: System musi aktualizować role i uprawnienia użytkowników po przypisaniu administratora.*

*REQ-36: System musi rejestrować wszystkie działania związane z tworzeniem organizacji i przypisywaniem administratorów do celów audytu.*

## Integracja aplikacji mobilnych

4.10.1 Opis i priorytet

*Ta funkcja obejmuje dedykowane aplikacje na systemy iOS i Android, które ułatwiają uwierzytelnianie użytkownika i bezpieczne przesyłanie danych do punktu wejścia za pośrednictwem NFC. Wysoki priorytet.*

4.10.2 Sekwencje / Odpowiedzi

*Użytkownik uruchamia aplikację mobilną i inicjuje proces logowania. System uwierzytelnia użytkownika i zapewnia dostęp do funkcji aplikacji. Użytkownik zbliża się do punktu wejścia ze swoim smartfonem, aby przesłać dane. System bezpiecznie przesyła dane użytkownika do punktu dostępu za pośrednictwem NFC.*

4.10.3 Wymagania funkcjonalne

*REQ-37: System musi zawierać aplikacje iOS i Android, które obsługują uwierzytelnianie użytkownika.*

*REQ-38: Aplikacje mobilne muszą bezpiecznie przesyłać dane użytkownika do punktu wejścia za pomocą technologii NFC.*

*REQ-39: Aplikacje mobilne muszą zapewniać przyjazny dla użytkownika interfejs do inicjowania transferu danych do punktu wejściowego.*

*REQ-40: System musi zapewniać szyfrowanie i bezpieczeństwo transferu danych podczas transakcji NFC.*

## Wizualizacja wyników akcji

4.11.1 Opis i priorytet

*Ta funkcja zapewnia użytkownikom wizualną informację zwrotną dotyczącą wyniku ich żądań dostępu, takich jak pomyślne wejście lub odmowa dostępu. Średni priorytet.*

4.11.2 Sekwencje / Odpowiedzi

*Użytkownik próbuje uzyskać dostęp do zabezpieczonego obszaru za pomocą smartfona. System przetwarza żądanie dostępu i określa wynik. Użytkownik czeka na informację zwrotną o wyniku żądania dostępu. System wyświetla powiadomienie wizualne wskazujące wynik żądania dostępu.*

4.11.3 Wymagania funkcjonalne

*REQ-41: System musi zapewniać wizualne powiadomienia dla użytkowników dotyczące statusu ich wniosków o dostęp.*

*REQ-42: System musi zapewniać, że powiadomienia są jasne i łatwo zrozumiałe dla użytkowników.*

*REQ-43: System musi rejestrować wizualne informacje zwrotne przekazywane użytkownikom do celów audytu i rozwiązywania problemów.*

## Obsługa błędów i reakcje na scenariusze

4.12.1 Opis i priorytet

*Ta funkcja umożliwia systemowi śledzenie i reagowanie na różne scenariusze błędów, takie jak nieudane transfery NFC lub próby nieautoryzowanego dostępu. Średni priorytet.*

4.12.2 Sekwencje / Odpowiedzi

*Użytkownik doświadcza nieudanego transferu NFC lub nieautoryzowanej próby dostępu. System wykrywa scenariusz błędu i uruchamia odpowiednie procedury obsługi błędów. Użytkownik może zgłosić błąd lub poprosić o pomoc. System zapewnia użytkownikowi wskazówki lub działania naprawcze, jeśli to możliwe, i rejestruje błąd w celu dalszej analizy.*

4.12.3 Wymagania funkcjonalne

*REQ-44: System musi wykrywać i rejestrować różne scenariusze błędów, w tym nieudane transfery NFC i próby nieautoryzowanego dostępu.*

*REQ-45: System musi zapewniać odpowiednie reakcje na scenariusze błędów, takie jak odmowa dostępu lub monit o podjęcie działań naprawczych.*

*REQ-46: System musi powiadamiać uprzywilejowanych użytkowników lub administratorów o istotnych scenariuszach błędów w celu ich sprawdzenia i rozwiązania.*