**Temat**: Scentralizowany system do autentykacji biometrycznej

**Autor:**

Jamroz Mateusz

Spis treści

* [Plan Projektu](#PLan)
* [Przypadki użycia](#Przypadki)
* [Wymagania](#Wymagania)
* [BPMN](#BPMN)
* [Diagramy przypadków użycia](#Diagramy)
* [User Stories](#User)
* [Diagram bazy danych ERD](#diagram)
* [Architektura](#architektura)
* [Wykres Gantta](#planmipl)
* [Analiza Ryzyka](#analizaryzyka)

Plan projektu

Projekt systemu przeznaczony do generycznej i scentralizowanej autentykacji biometrycznej pozwalającej firmom na dowolne nadawanie uprawnień w zależności od przypisania do danej placówki. Jest to rozwiązanie rewolucyjne, ponieważ obecnie na rynku nie ma takiego rozwiązania, a te co są nie oferują tak zaawansowanych i wygodnych możliwości. Produkt ten będzie upraszczał życie kierownikom, pracodawcom, ale najbardziej zwyczajnym osobom, które poprzez zwykłe dodanie swoich zdjęć i odcisków palca, będą miały możliwość autoryzowania się wszędzie tam, gdzie będą miały dostęp. Jedna rejestracja i weryfikacja, wiele użyć.

Pracodawcy będą mieli możliwość wykupienia usług na zasadzie montażu jak i opłaty za świadczone usługi w zależności od zakresu i ilości wspieranych możliwości autoryzacji.

Dla użytkowników będzie darmowy dostęp do aplikacji mobilnej i webowej, pozwalającej na dodanie swoich danych osobowych do weryfikacji jak i późniejsze modyfikowanie ich.

Do wykonania projektu wymagane będzie użycie chmury (lub serwera), na którym będzie możliwość uruchomienia poszczególnych komponentów napisanych w technologiach: react, spring boot, flask, oraz systemu bazodanowego postgresql. Również do 100% integracji będzie wymagana licencja android developer i IOS developer, z poprawnymi zasadami regulaminu.  
Od użytkownika wymagane będzie przeglądarka zgodna HTML5, CSS, Javascript, oraz telefon IOS / Android.

Cel projektu -> zgodnie z metodologią S.M.A.R.T (pol. Z.M.O.R.A – Zdefiniowanie, Mierzalne, Ograniczenie w czasie, Realne, Akceptowalne)

Naszym głównym celem jest realizacja i wdrożenie pomysłu, którego obecnie nie ma na rynku a by stanowił znakomite rozszerzenie dla platform typu **Multisport**, oraz **Medicover Sport**, co nie zmienia faktu, że system ten idealnie wpasowuje się dla mniejszych przedsiębiorstw.

Celem bezpośrednim, którym zamierzamy osiągnąć jest zdobycie tysiąca klientów w ciągu 3 miesięcy, od pierwszej prezentacji wersji testowej, oraz zapewnienie kosztów utrzymania i dalszego developmentu. Alternatywą jest współpraca z większą korporacją, która zagwarantuje wystarczający budżet, oraz klientów.

Pierwszą wersję aplikacji chcemy móc przedstawić na przestrzeni 3 miesięcy. W tym czasie chcielibyśmy osiągnąć wysoką pozycję w wyszukiwarce **Google**, oraz wysoką pozycję w sklepie play, ewentualna integracja z istniejącą aplikacją typu **Multisport.**

Budżet niezbędny do realizacji pierwszych faz projektu to jedynie koszt chmury, oraz domeny (59,99 zł i 399,00 zł rocznie), ponieważ zespół zgodził się wziąć udział w przedsięwzięciu procentowo od zysków. W ciągu roku powinna powstać w pełni funkcjonalna aplikacja, po fazach testów, oraz dostosowana do potrzeb użytkowników

W pierwszej fazie zakładamy, że głównymi użytkownikami, będą młode osoby aktywnie korzystające z placówek, potrzebujących autoryzacji (np. siłownie). W pierwszym cyklu celem jest udostępnienie autoryzacji poprzez odcisk palca, oraz twarzy.

Uważamy, że młode osoby, które będą korzystały z siłowni, z wielką chęcią będą korzystały z naszego systemu, gdyż znacząco uprości i uprzyjemni im życie.

Będziemy także badać wykorzystanie funkcji i przyjmować opinie od naszych użytkowników, aby odpowiednio reagować na rzecz poprawy jakości naszego produktu.

Gdy aplikacja stanie się bardziej dojrzała będziemy skupiać się na markecie, gdzie używamy poświadczeń, że jesteśmy sobą. Następnie zaimplementować specjalne rozwiązania, oraz urządzenia dla potrzeb klientów.

|  |  |  |
| --- | --- | --- |
| Nazwa | Opis | Rodzaj |
| Niezarejestrowany użytkownik | Aktor nie posiadający praw korzystania z usług systemu. Może przeglądać stronę główną, a także zarejestrować/zalogować się. | Osoba |
| Zarejestrowany użytkownik | Aktor mogący korzystać z podstawowych usług systemu, aplikować do innych palcówek, przesyłać oraz edytować swoje dane wrażliwe, przeglądać historię wejść, oraz otrzymywać powiadomienia. | Osoba |
| Właściciel placówki / Admin | Aktor posiada możliwość edytowania przynależnych aktorów do danej placówki, przeglądać całkowitą historię wejść, | Osoba |
| System Owner | Owner ma całkowitą możliwość edycji danych placówek, zarządzania przynależnością użytkowników oraz możliwość edycji wspieranych produktów. | Osoba |
| System Autoryzacji | Jego zadaniem jest wykorzystanie sztucznej inteligencji, jako rozwiązania do jednoznacznej identyfikacji danej osoby, a następnie sprawdzenie jej przynależności. | System |
| Urządzenia autoryzujące | Jego zadaniem jest wysłaniue zapytania na serwer, a następnie wywołanie konsekwentnych akcji do umożliwienia pomyślnego procesu weryfikacji od strony sprzętowej. | Urządzenie |

Przypadki użycia

**UC001: Rejestracja w systemie**

Aktorzy: Niezarejestrowany użytkownik

Scenariusz główny:

Niezarejestrowany użytkownik otwiera stronę główną systemu.

Użytkownik wybiera opcję rejestracji.

System prezentuje formularz rejestracyjny z polami do wprowadzenia danych.

Użytkownik wprowadza wymagane dane, takie jak login, hasło, adres e-mail.

Użytkownik zatwierdza wprowadzone dane.

System rejestruje użytkownika i przypisuje mu rolę zarejestrowanego użytkownika.

Użytkownik zostaje przekierowany do strony logowania.

Koniec przypadku użycia.

Rozszerzenia:

4A. Użytkownik wprowadza nieprawidłowe dane rejestracyjne

4A1. System wyświetla komunikat o błędzie i prosi o ponowne wprowadzenie poprawnych danych.

4A2. Użytkownik poprawia dane i wraca do kroku 5 scenariusza głównego.

4B. Użytkownik posiada już konto i chce wrócić do strony logowania

4B1. Użytkownik klika opcję powrotu.

4B2. System przekierowuje użytkownika do strony logowania.

4B3. Koniec przypadku użycia.

**UC002: Przeglądanie Strony Głównej**

Aktorzy: Niezarejestrowany użytkownik

Scenariusz główny:

Niezarejestrowany użytkownik otwiera stronę główną systemu.

System wyświetla ogólną zawartość strony głównej, zawierającą podstawowe informacje o usługach, produktach lub aktualnościach.

Użytkownik przegląda dostępne treści, takie jak nagłówki, grafiki i krótkie opisy.

Niezarejestrowany użytkownik może dowiedzieć się o ogólnych funkcjach systemu oraz zobaczyć informacje zachęcające do rejestracji.

Koniec przypadku użycia.

Rozszerzenia:

2A. Użytkownik chce przejść do procesu rejestracji

2A1. Użytkownik klika przycisk "Zarejestruj się".

2A2. System przenosi użytkownika do formularza rejestracyjnego (patrz UC001).

2A3. Koniec przypadku użycia.

2B. Użytkownik chce przejść do procesu logowania

2B1. Użytkownik klika przycisk "Zaloguj się".

2B2. System przenosi użytkownika do formularza logowania.

2B3. Koniec przypadku użycia.

**UC003: Edycja Danych Wrażliwych**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Zarejestrowany użytkownik loguje się do systemu.

Użytkownik przechodzi do panelu ustawień konta.

System prezentuje formularz z aktualnymi danymi wrażliwymi użytkownika, używanymi do autoryzacji

Użytkownik wprowadza zmiany w polach, które chce zaktualizować.

Użytkownik zatwierdza wprowadzone zmiany.

System aktualizuje dane wrażliwe użytkownika.

Użytkownik otrzymuje potwierdzenie zaktualizowania danych.

Koniec przypadku użycia.

Rozszerzenia:

4A. Użytkownik nie zatwierdza zmian

4A1. System wyświetla komunikat, informujący użytkownika o konieczności potwierdzenia zmian.

4A2. Użytkownik decyduje się albo potwierdzić, albo anulować wprowadzone zmiany.

4A3. Powrót do kroku 3 scenariusza głównego.

4B. Użytkownik wprowadza nieprawidłowe dane

4B1. System wyświetla komunikat o błędzie i prosi o ponowne wprowadzenie poprawnych danych.

4B2. Użytkownik poprawia dane i zatwierdza zmiany.

4B3. Koniec przypadku użycia.

**UC004: Aplikowanie do Placówki**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Zarejestrowany użytkownik loguje się do systemu.

Użytkownik przegląda dostępne placówki i oferty pracy.

System prezentuje listę dostępnych placówek oraz ofert pracy w każdej z nich.

Użytkownik wybiera konkretną placówkę lub ofertę, do której chce aplikować.

System wyświetla formularz aplikacyjny z polami do wprowadzenia danych, takich jak doświadczenie, umiejętności, czy załącznik CV.

Użytkownik wprowadza wymagane dane i dołącza niezbędne dokumenty.

Użytkownik zatwierdza aplikację.

System rejestruje aplikację użytkownika i przekazuje ją do oceny placówki.

Użytkownik otrzymuje potwierdzenie złożenia aplikacji.

Koniec przypadku użycia.

Rozszerzenia:

4A. Użytkownik chce wrócić do listy placówek

4A1. Użytkownik klika przycisk powrotu.

4A2. System przekierowuje użytkownika z powrotem do listy placówek.

4A3. Koniec przypadku użycia.

6A. Użytkownik nie dołącza wymaganych dokumentów

6A1. System informuje użytkownika o konieczności dołączenia wymaganych dokumentów.

6A2. Użytkownik dodaje odpowiednie załączniki i ponownie zatwierdza aplikację.

6A3. Powrót do kroku 8 scenariusza głównego.

**UC004: Przeglądanie Historii Wejść**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Zarejestrowany użytkownik loguje się do systemu.

Użytkownik przechodzi do panelu swojego konta lub historii wejść.

System prezentuje listę ostatnich wejść użytkownika do systemu.

Użytkownik przegląda szczegóły historii wejść, takie jak data, godzina, miejsce logowania.

Koniec przypadku użycia.

Rozszerzenia:

2A. Użytkownik chce przeglądać bardziej szczegółową historię wejść

2A1. Użytkownik klika na konkretny wpis w historii.

2A2. System wyświetla szczegółowe informacje, takie jak adres IP, urządzenie, przeglądarka itp.

2A3. Użytkownik przegląda dodatkowe informacje i wraca do ogólnej historii wejść.

2A4. Koniec przypadku użycia.

2B. Użytkownik chce wylogować się z systemu

2B1. Użytkownik klika przycisk wylogowania.

2B2. System zamyka sesję użytkownika, wylogowując go z systemu.

2B3. Koniec przypadku użycia.

**UC005: Przeglądanie Powiadomień**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Zarejestrowany użytkownik loguje się do systemu.

Użytkownik przechodzi do panelu powiadomień lub ikony z powiadomieniami.

System prezentuje listę najnowszych powiadomień użytkownika.

Użytkownik przegląda zawartość powiadomień, zawierającą informacje o nowych zdarzeniach, wiadomościach czy aktualizacjach.

Koniec przypadku użycia.

Rozszerzenia:

2A. Użytkownik chce przeczytać pełną treść powiadomienia

2A1. Użytkownik klika na konkretny tytuł lub treść powiadomienia.

2A2. System wyświetla pełną treść powiadomienia z dodatkowymi informacjami.

2A3. Użytkownik czyta pełne powiadomienie i wraca do listy powiadomień.

2A4. Koniec przypadku użycia.

2B. Użytkownik chce oznaczyć powiadomienia jako przeczytane

2B1. Użytkownik korzysta z opcji oznaczania jako przeczytane.

2B2. System aktualizuje status powiadomień, oznaczając je jako przeczytane.

2B3. Koniec przypadku użycia.

**UC006: Dodawanie Metody Autoryzacji**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Zarejestrowany użytkownik loguje się do systemu.

Użytkownik przechodzi do panelu ustawień konta.

System prezentuje opcje związane z autoryzacją i bezpieczeństwem konta.

Użytkownik wybiera opcję "Dodaj metodę autoryzacji".

System wyświetla dostępne metody autoryzacji, takie jak dwuskładnikowa autoryzacja, kod SMS itp.

Użytkownik wybiera preferowaną metodę autoryzacji.

Zgodnie z wybraną metodą, użytkownik wprowadza i potwierdza niezbędne informacje, takie jak numer telefonu czy klucz bezpieczeństwa.

System zapisuje dodaną metodę autoryzacji do konta użytkownika.

Użytkownik otrzymuje potwierdzenie dodania nowej metody autoryzacji.

Koniec przypadku użycia.

Rozszerzenia:

6A. Użytkownik chce anulować dodawanie metody autoryzacji

6A1. Użytkownik kliknie przycisk "Anuluj".

6A2. System zatrzymuje proces dodawania metody autoryzacji.

6A3. Koniec przypadku użycia.

7A. Użytkownik wprowadza nieprawidłowe dane autoryzacji

7A1. System wyświetla komunikat o błędzie i prosi o poprawienie danych.

7A2. Użytkownik poprawia dane i ponownie potwierdza dodawanie metody autoryzacji.

7A3. Powrót do kroku 9 scenariusza głównego.

**UC007: Powiadomienie o Uczeniu się AI na Danych Użytkownika**

Aktorzy: Zarejestrowany użytkownik

Scenariusz główny:

Użytkownik jest zalogowany do systemu.

System automatycznie analizuje i uczy się z dostępnych danych użytkownika przy użyciu sztucznej inteligencji.

Użytkownik otrzymuje powiadomienie o procesie uczenia się AI na jego danych.

Powiadomienie zawiera informacje o celu uczenia się, rodzaju danych używanych oraz ochronie prywatności.

Użytkownik ma opcję zapoznania się z więcej szczegółami dotyczącymi procesu uczenia się AI.

Użytkownik może wyrazić zgodę lub zrezygnować z udziału w procesie uczenia się na swoich danych.

Koniec przypadku użycia.

Rozszerzenia:

3A. Użytkownik chce uzyskać więcej informacji

3A1. Użytkownik kliknie na link lub przycisk "Więcej informacji".

3A2. System wyświetli szczegółowe informacje dotyczące procesu uczenia się AI na danych użytkownika.

3A3. Użytkownik może ponownie podjąć decyzję o zgodzie lub rezygnacji.

3A4. Powrót do kroku 5 scenariusza głównego.

6B. Użytkownik decyduje się zrezygnować z udziału w procesie uczenia się

6B1. Użytkownik korzysta z opcji rezygnacji.

6B2. System respektuje decyzję użytkownika i nie używa jego danych do procesu uczenia się AI.

6B3. Koniec przypadku użycia.

**UC008: Przeglądanie Panelu Administracyjnego**

Aktorzy: Właściciel placówki / Admin

Scenariusz główny:

Właściciel placówki lub administrator loguje się do systemu.

Użytkownik przechodzi do panelu administracyjnego.

System prezentuje zestawienie kluczowych informacji dotyczących placówki, takich jak statystyki, lista zarejestrowanych użytkowników, aktywne oferty pracy itp.

Właściciel placówki może przeglądać i edytować dane dotyczące pracowników oraz dostosowywać ustawienia placówki.

Administrator może także zarządzać kontami innych użytkowników przypisanych do placówki.

Właściciel placówki ma dostęp do raportów i analiz dotyczących aktywności oraz efektywności placówki.

Koniec przypadku użycia.

Rozszerzenia:

4A. Właściciel placówki chce dodać nowego pracownika

4A1. Właściciel placówki wybiera opcję dodania nowego pracownika.

4A2. System prezentuje formularz z danymi do wprowadzenia.

4A3. Właściciel placówki wprowadza niezbędne informacje i zatwierdza dodanie nowego pracownika.

4A4. Koniec przypadku użycia.

4B. Administrator chce zablokować konto użytkownika

4B1. Administrator wybiera opcję zarządzania kontami użytkowników.

4B2. System prezentuje listę użytkowników przypisanych do placówki.

4B3. Administrator wybiera konto do zablokowania i potwierdza operację.

4B4. Konto użytkownika zostaje zablokowane, a administrator otrzymuje potwierdzenie.

4B5. Koniec przypadku użycia.

**UC009: Dodawanie i Edytowanie Użytkowników w Placówce**

Aktorzy: Właściciel placówki / Admin

Scenariusz główny:

Właściciel placówki lub administrator loguje się do systemu.

Użytkownik przechodzi do panelu administracyjnego placówki.

System prezentuje opcje zarządzania użytkownikami przypisanymi do danej placówki.

Właściciel placówki wybiera opcję "Dodaj nowego użytkownika".

System wyświetla formularz z danymi do wprowadzenia dla nowego użytkownika.

Właściciel placówki wprowadza niezbędne informacje, takie jak imię, nazwisko, adres e-mail, oraz przydziela odpowiednie role.

Właściciel placówki zatwierdza dodanie nowego użytkownika do placówki.

System rejestruje nowego użytkownika i aktualizuje listę przypisanych do placówki.

Właściciel placówki otrzymuje potwierdzenie dodania nowego użytkownika.

Rozszerzenia:

10A. Właściciel placówki chce edytować istniejącego użytkownika

10A1. Właściciel placówki wybiera opcję "Edytuj użytkownika".

10A2. System prezentuje formularz z aktualnymi danymi użytkownika.

10A3. Właściciel placówki dokonuje niezbędnych edycji, takich jak zmiana roli czy aktualizacja danych osobowych.

10A4. Właściciel placówki zatwierdza wprowadzone zmiany.

10A5. System aktualizuje dane użytkownika w placówce.

10A6. Właściciel placówki otrzymuje potwierdzenie edycji użytkownika.

**UC010: Przeglądanie Historii Wejść w Placówce**

Aktorzy: Właściciel placówki / Admin

Scenariusz główny:

Właściciel placówki lub administrator loguje się do systemu.

Użytkownik przechodzi do panelu administracyjnego placówki.

System prezentuje opcje zarządzania placówką, w tym historię wejść.

Właściciel placówki wybiera opcję "Historia Wejść".

System prezentuje listę ostatnich wejść użytkowników do placówki, zawierającą informacje takie jak data, godzina, miejsce logowania.

Właściciel placówki może przeglądać szczegóły historii wejść dla różnych użytkowników.

Koniec przypadku użycia.

Rozszerzenia:

5A. Właściciel placówki chce uzyskać więcej szczegółów

5A1. Właściciel placówki klika na konkretny wpis w historii.

5A2. System wyświetla szczegółowe informacje, takie jak adres IP, urządzenie, przeglądarka itp.

5A3. Właściciel placówki przegląda dodatkowe informacje i wraca do ogólnej historii wejść.

5A4. Koniec przypadku użycia.

**UC011: Monitorowanie Wejść w Czasie Rzeczywistym w Placówce**

Aktorzy: Właściciel placówki / Admin

Scenariusz główny:

Właściciel placówki lub administrator loguje się do systemu.

Użytkownik przechodzi do panelu administracyjnego placówki.

System prezentuje opcje monitorowania placówki, w tym monitorowanie wejść w czasie rzeczywistym.

Właściciel placówki wybiera opcję "Monitorowanie Wejść w Czasie Rzeczywistym".

System uruchamia interaktywny panel, przedstawiający bieżącą aktywność wejść do placówki.

Właściciel placówki może obserwować na bieżąco, kto wchodzi do placówki, o której godzinie i z jakiego miejsca.

System aktualizuje dane w czasie rzeczywistym, umożliwiając właścicielowi placówki natychmiastowe reagowanie na zmiany.

Koniec przypadku użycia.

Rozszerzenia:

5A. Właściciel placówki chce uzyskać dodatkowe informacje o konkretnym wejściu

5A1. Właściciel placówki klika na konkretny wpis w panelu monitorowania.

5A2. System dostarcza dodatkowe informacje, takie jak szczegóły użytkownika, czas trwania wejścia itp.

5A3. Właściciel placówki może podjąć decyzje na podstawie dodatkowych informacji.

5A4. Koniec przypadku użycia.

**UC012: Przeglądanie i Zmiana Profilu Właściciela Placówki**

Aktorzy: Właściciel placówki / Admin

Scenariusz główny:

Właściciel placówki lub administrator loguje się do systemu.

Użytkownik przechodzi do panelu swojego konta lub ustawień profilu.

System prezentuje informacje dotyczące profilu właściciela placówki, takie jak imię, nazwisko, dane kontaktowe itp.

Właściciel placówki może przeglądać aktualne dane swojego profilu.

Właściciel placówki wybiera opcję "Edytuj Profil".

System umożliwia wprowadzenie zmian w danych profilu, takich jak zmiana danych kontaktowych czy adresu e-mail.

Właściciel placówki zatwierdza wprowadzone zmiany.

System aktualizuje dane profilu właściciela placówki.

Właściciel placówki otrzymuje potwierdzenie zaktualizowania danych.

Koniec przypadku użycia.

Rozszerzenia:

6A. Właściciel placówki chce zmienić hasło dostępu

6A1. Właściciel placówki wybiera opcję "Zmień Hasło".

6A2. System przeprowadza proces zmiany hasła, wymagając od właściciela placówki podania obecnego hasła oraz wprowadzenia nowego.

6A3. Właściciel placówki zatwierdza zmiany hasła.

6A4. Koniec przypadku użycia.

**UC013: Dodawanie Placówki przez System Owner**

Aktorzy: System Owner

Scenariusz główny:

System Owner loguje się do systemu jako użytkownik o uprawnieniach System Owner.

System prezentuje panel administracyjny System Owner z dostępem do zarządzania placówkami.

System Owner wybiera opcję "Dodaj nową placówkę".

System wyświetla formularz z danymi do wprowadzenia dla nowej placówki, takimi jak nazwa, adres, dane kontaktowe.

System Owner wprowadza niezbędne informacje i zatwierdza dodanie nowej placówki.

System rejestruje nową placówkę i przypisuje ją do listy placówek zarządzanych przez System Ownera.

System Owner otrzymuje potwierdzenie dodania nowej placówki.

Koniec przypadku użycia.

Rozszerzenia:

4A. System Owner chce przypisać właściciela do nowej placówki

4A1. System prezentuje opcję wyboru właściciela dla nowej placówki.

4A2. System Owner wybiera właściciela z listy użytkowników lub dodaje nowego właściciela.

4A3. System przypisuje właściciela do nowej placówki.

4A4. Powrót do kroku 5 scenariusza głównego.

4B. System Owner chce anulować dodawanie nowej placówki

4B1. System Owner kliknie przycisk "Anuluj".

4B2. System zatrzymuje proces dodawania nowej placówki.

4B3. Koniec przypadku użycia.

**UC014: Przeglądanie System Owner Panelu**

Aktorzy: System Owner

Scenariusz główny:

System Owner loguje się do systemu jako użytkownik o uprawnieniach System Owner.

System prezentuje panel administracyjny System Owner z dostępem do zarządzania różnymi aspektami systemu.

System Owner ma dostęp do informacji dotyczących wszystkich placówek, użytkowników i innych elementów systemu.

System Owner może przeglądać statystyki, raporty oraz ogólne informacje dotyczące funkcjonowania systemu.

System Owner ma możliwość zarządzania uprawnieniami innych użytkowników, w tym nadawania lub odbierania roli System Owner.

System Owner może korzystać z narzędzi administracyjnych do monitorowania aktywności systemu oraz podejmowania decyzji o zmianach czy ulepszeniach.

Koniec przypadku użycia.

**UC015: Przeglądanie Użytkowników i Ich Przypisania do Placówki przez System Ownera**

Aktorzy: System Owner

Scenariusz główny:

System Owner loguje się do systemu jako użytkownik o uprawnieniach System Owner.

System prezentuje panel administracyjny System Ownera z dostępem do zarządzania użytkownikami i przypisaniami do placówek.

System Owner wybiera opcję "Przeglądaj Użytkowników i Ich Przypisania do Placówki".

System wyświetla listę wszystkich użytkowników systemu wraz z informacjami dotyczącymi ich ról i przypisania do placówek.

System Owner ma możliwość filtrowania użytkowników według różnych kryteriów, takich jak rola, nazwa placówki, itp.

System Owner może przeglądać szczegóły poszczególnych użytkowników, w tym ich dane osobowe i historię aktywności.

System Owner może edytować przypisanie użytkownika do konkretnej placówki, zmieniać role lub usuwać użytkowników z przypisania.

Koniec przypadku użycia.

Rozszerzenia:

5A. System Owner chce przypisać nowego użytkownika do placówki

5A1. System Owner wybiera opcję "Przypisz nowego użytkownika do placówki".

5A2. System prezentuje formularz z danymi do wprowadzenia dla nowego użytkownika, a także opcje przypisania do konkretnej placówki i nadania roli.

5A3. System Owner wprowadza niezbędne informacje i zatwierdza przypisanie nowego użytkownika do placówki.

5A4. System aktualizuje listę użytkowników i ich przypisań do placówek.

5A5. Koniec przypadku użycia.

7A. System Owner chce usunąć użytkownika z przypisania do placówki

7A1. System Owner wybiera opcję "Usuń użytkownika z przypisania do placówki".

7A2. System potwierdza decyzję i usuwa użytkownika z przypisania do danej placówki.

7A3. System aktualizuje listę użytkowników i ich przypisań do placówek.

7A4. Koniec przypadku użycia.

**UC016: Zmiana Nazwy Placówki przez System Ownera**

Aktorzy: System Owner

Scenariusz główny:

System Owner loguje się do systemu jako użytkownik o uprawnieniach System Owner.

System prezentuje panel administracyjny System Ownera z dostępem do zarządzania placówkami.

System Owner wybiera opcję "Zarządzaj Placówkami".

System prezentuje listę placówek z informacjami, w tym ich aktualnymi nazwami.

System Owner wybiera placówkę, której nazwę chce zmienić.

System prezentuje formularz umożliwiający wprowadzenie nowej nazwy dla placówki.

System Owner wprowadza nową nazwę placówki i zatwierdza zmiany.

System aktualizuje nazwę placówki w systemie.

System Owner otrzymuje potwierdzenie zmiany nazwy placówki.

Koniec przypadku użycia.

Rozszerzenia:

5A. System Owner chce anulować zmianę nazwy placówki

5A1. System Owner wybiera opcję "Anuluj".

5A2. System zatrzymuje proces zmiany nazwy placówki.

5A3. Brak zmian w nazwie placówki.

5A4. Koniec przypadku użycia.

Wymagania

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Tytuł | Opis | Use Case |
| 1 | Autoryzacja biometryczna | System zapewnia funkcjonalności i komponenty niezbędne do autoryzacji biometrycznej | U003 |
| 2 | Autoryzacja systemowa | Użytkownik ma możliwość zalogowania się do systemu przy użyciu własnego konta | UC001  UC003 |
| 3 | Rejestracja placówki | System zapewnia możliwość rejestracji placówki, oraz ewentualnego rozpatrzenia wniosku | UC004  UC010  UC013 |
| 4 | Rejestracja użytkownika | Użytkownik ma możliwość na zarejestrowanie się i utworzenie konta | UC001 |
| 5 | Przeglądanie wejść | Osoba ma możliwość przeglądania historii wejść | UC005  UC004 |
| 6 | Edycja danych wrażliwych | Użytkownik ma możliwość edycji swoich danych wrażliwych dla danej metody autoryzacji | UC003 |
| 7 | Modyfikacja usług produktowych | Lokalni i Główni administratorzy mają możliwość modyfikacji określonych usług | U0015 |
| 8 | Zarządzanie użytkownikami (lokalnie) | Lokalni administratorzy mając możliwość modyfikacji przynależności użytkowników | UC003 |
| 9 | Zarządzanie użytkownikami (admin) | Główni administratorzy mają możliwość całkowitej modyfikacji użytkowników | UC003 |
| 10 | Zarządzanie placówką (lokalnie) | Lokalni administratorzy mają możliwość modyfikacji własności własnej placówki | UC008  UC009 |
| 11 | Zarządzanie placówką (admin) | Główni administratorzy mają możliwość ograniczonego zarządzania wszystkimi placówkami | UC012  UC014  UC015 |

BPMN

Obraz zawierający tekst, diagram, linia, Czcionka

Opis wygenerowany automatycznie

Diagramy przypadków użycia

Obraz zawierający tekst, diagram, zrzut ekranu, linia

Opis wygenerowany automatycznie

User Stories

Jako: Niezarejestrowany użytkownik

Chcę: Utworzyć konto

Aby: Mieć dostęp do aplikacji

Scenariusz: UC001

Jako: Niezarejestrowany użytkownik

Chcę: Przeglądać ofertę firmy oraz stronę główną

Aby: Dowiedzieć się o ogólnych funkcjach systemu oraz zobaczyć informacje zachęcające do rejestracji

Scenariusz: UC002

Jako: Zarejestrowany użytkownik

Chcę: Mieć możliwość aplikowania do placówki

Aby: Móc dołączyć do placówki i skorzystać z ofert pracy

Scenariusz: UC003

Jako: Zarejestrowany użytkownik

Chcę: Mieć możliwość edytowania danych wrażliwych

Aby: Mieć aktualne i bezpieczne dane do autoryzacji

Scenariusz: UC005

Jako: Zarejestrowany użytkownik

Chcę: Składać wnioski o przynależność do danej placówki

Aby: Móc formalnie należeć do placówki i korzystać z jej usług

Scenariusz: UC004

Jako: Zarejestrowany użytkownik

Chcę: Mieć możliwość dodania metody autoryzacji

Aby: Zwiększyć bezpieczeństwo dostępu do mojego konta

Scenariusz: UC006

Jako: Zarejestrowany użytkownik

Chcę: Być informowanym o uczeniu się AI na moich danych

Aby: Mieć świadomość i kontrolę nad wykorzystaniem moich danych

Scenariusz: UC007

Jako: Właściciel placówki / Admin

Chcę: Przeglądać panel administracyjny

Aby: Zarządzać kluczowymi informacjami dotyczącymi placówki

Scenariusz: UC008

Jako: Właściciel placówki / Admin

Chcę: Dodawać i edytować użytkowników przypisanych do placówki

Aby: Zarządzać składem personalnym placówki

Scenariusz: UC009

Jako: Właściciel placówki / Admin

Chcę: Przeglądać historię wejść w placówce

Aby: Monitorować aktywność użytkowników

Scenariusz: UC010

Jako: Właściciel placówki / Admin

Chcę: Monitorować wejścia w czasie rzeczywistym

Aby: Być na bieżąco z aktywnością w placówce

Scenariusz: UC011

Jako: Właściciel placówki / Admin

Chcę: Przeglądać i zmieniać mój profil właściciela placówki

Aby: Aktualizować moje dane kontaktowe i zarządcze

Scenariusz: UC012

Jako: System Owner

Chcę: Dodawać nową placówkę

Aby: Rozszerzać sieć placówek systemu

Scenariusz: UC013

Jako: System Owner

Chcę: Przeglądać panel System Owner

Aby: Zarządzać różnymi aspektami systemu

Scenariusz: UC014

Jako: System Owner

Chcę: Przeglądać użytkowników i ich przypisania do placówek

Aby: Zarządzać relacjami użytkowników z placówkami

Scenariusz: UC015

Jako: System Owner

Chcę: Zmieniać nazwy placówek

Aby: Aktualizować informacje o placówkach zgodnie z potrzebami

Scenariusz: UC016

Diagramy bazy danych ERD

Obraz zawierający tekst, zrzut ekranu, diagram

Opis wygenerowany automatycznie

Architektura i wybór technologii

Architekturą dla tej aplikacji jest klient-serwer z użyciem mikroserwisów, ponieważ chciałbym rozdzielić stronę frontend – backend. Z racji, że rozwiązanie polega na użyciu dwóch rozbieżnych technologii, to wydajność między serwisami może być słaba, stąd moim wyborem będzie platforma streamingowa typu kafka.

Technologia wybrana dla projektu to:

- Spring Boot to framework do budowania aplikacji w języku Java, umożliwiający szybkie i efektywne tworzenie mikroserwisów.

- PostgreSQL to system zarządzania relacyjnymi bazami danych, charakteryzujący się wydajnością i skalowalnością.

- Angular.js to biblioteka JavaScript do budowania interfejsów użytkownika, umożliwiająca dynamiczne i efektywne tworzenie interaktywnych stron internetowych.

- Kafka to platforma do przesyłania strumieniowego danych, zapewniająca skalowalność i odporność na awarie.

- TensorFlow to biblioteka do uczenia maszynowego, wykorzystywana do budowy i treningu modeli sztucznej inteligencji.

- Flask, framework pozwalający na szybkie tworzenie API w pythonie

W połączeniu, te technologie umożliwiają kompleksowy rozwój projektu, łącząc backend, bazę danych, interfejs użytkownika, przetwarzanie strumieniowe danych i uczenie maszynowe.

Plan Implementacji – Wykres Gantta

Obraz zawierający tekst, paragon, numer

Opis wygenerowany automatycznie

Analiza Ryzyka

| **Lp.** | **Zagrożenie** | **Wielkość szkody (S)** | **Prawdopodobieństwo powstania szkody (P)** | **Ryzyko (W): W=SxP** |
| --- | --- | --- | --- | --- |
| 1 | Nieautoryzowany dostęp do danych wrażliwych przez błąd w zarządzaniu użytkownikami | Ciężkie szkody, S=4 | Dość prawdopodobne, raz na 5 lat, P=3 | W=12, wymaga działań naprawczych |
| 2 | Błędy w procesie rejestracji użytkownika pozwalające na rejestrację fałszywych kont | Średnie szkody, S=3 | Prawdopodobne, raz na rok, P=4 | W=12, wymaga działań naprawczych |
| 3 | Awaria systemu podczas dodawania metody autoryzacji, co może prowadzić do blokady konta | Średnie szkody, S=3 | Rzadko, raz na 3 lata, P=2 | W=6, dopuszczalna akceptacja ryzyka |
| 4 | Niewystarczające testowanie produktu przed wypuszczeniem może prowadzić do błędów | Średnie szkody, S=3 | Możliwe, raz na 2 lata, P=3 | W=9, dopuszczalna akceptacja ryzyka |
| 5 | Wyciek danych podczas aplikowania do placówki przez niezabezpieczone formularze | Ciężkie szkody, S=4 | Mało prawdopodobne, raz na 10 lat, P=2 | W=8, dopuszczalna akceptacja ryzyka |
| 6 | Niedostępność usług po wynajmie z powodu awarii serwerów | Średnie szkody, S=3 | Doraźne wydarzenia, raz na 2 lata, P=3 | W=9, dopuszczalna akceptacja ryzyka |
| 7 | Przeciążenie serwerów z powodu braku skalowalności przy masowej rejestracji użytkowników | Średnie szkody, S=3 | Rzadko, raz na 5 lat, P=2 | W=6, dopuszczalna akceptacja ryzyka |