# 1. Nazwa use case'u

Logowanie do aplikacji

# 2. Wstęp

Use case ten opisuje proces logowania

# 3. Cel use case'u

Celem jest autoryzacja, zapewnienie bezpieczeństwa, monitorowanie aktywności użytkowników oraz zwiększenie użyteczności aplikacji poprzez personalizację. Dzięki temu, tylko uprawnieni użytkownicy mają dostęp do funkcji i zasobów aplikacji, a aplikacja jest chroniona przed nieautoryzowanym dostępem.

# 4. Lista aktorów

* Klient zarejestrowany
* Klient niezarejestrowany

## 4.1 Aktor inicjujący

* Klient zarejestrowany
* Klient niezarejestrowany

## 4.2 Uczestnicy

# 5. Przebieg use case'u

Krok 1

Użytkownik wchodzi na ekran logowania

Krok 2

Wprowadza swoje dane logowania (np. login i hasło)

Krok 3

Aplikacja sprawdza poprawność danych logowania

Krok 4

Jeśli dane są poprawne, użytkownik zostaje zalogowany do aplikacji

Krok 5

W przypadku błędnych danych, aplikacja może wyświetlić komunikat o niepoprawności danych

Krok 6

Użytkownik może próbować ponownie wprowadzić poprawne dane lub skorzystać z funkcji przywracania hasła

Krok 7

Po zalogowaniu użytkownik ma dostęp do pełnej funkcjonalności aplikacji

# 6. Wyjątki

1. Błędne dane logowania: Użytkownik podaje niepoprawny login lub hasło. Aplikacja może wykryć niezgodność między podanymi danymi a danymi przechowywanymi w systemie i wyświetlić komunikat o błędnych danych logowania. Użytkownik może spróbować ponownie wprowadzić poprawne dane lub skorzystać z funkcji przywracania hasła.

2. Konto nieaktywne: Jeśli konto użytkownika jest nieaktywne, aplikacja może nie zezwolić na zalogowanie się do aplikacji. Może wyświetlić komunikat informujący o konieczności aktywacji konta przed uzyskaniem dostępu do aplikacji. Użytkownik może być skierowany do procedury aktywacji konta, takiej jak potwierdzenie adresu e-mail.

3. Zapomniane hasło: Jeśli użytkownik zapomni swoje hasło, może skorzystać z funkcji przywracania hasła. Aplikacja może udostępnić odpowiednią procedurę, taką jak resetowanie hasła za pomocą linka wysłanego na zarejestrowany adres e-mail użytkownika.

# 7. Przebiegi alternatywne

*<Przebieg Alternatywny 1>*

*[W tej części use case'u należy podać listę i przebieg alternatywny dla use case’u. Opis przebiegu alternatywnego powinien być zapisany w formie numerowanych zdań. Pierwsze zdanie w opisie alternatywnym powinno mieć numer zdania z głównego przebiegu use case'u od którego zaczyna się przebieg alternatywny. Jeżeli przebieg alternatywny jest dostatecznie długo można zawrzeć go w osobnym use case‘ie i podać do niego referencje.]*

# 8. Zagadnienia implementacyjne

Weryfikacja danych logowania - system musi zweryfikować, czy wprowadzone przez użytkownika dane logowania są poprawne, przed udzieleniem dostępu do aplikacji.

Synchronizacja z bazą danych - system musi być w stanie zsynchronizować dane logowania z bazą danych, w celu weryfikacji tożsamości użytkownika.

Zapamiętanie sesji - system może zapamiętywać sesje użytkownika, aby użytkownik nie musiał wprowadzać danych logowania przy każdym uruchomieniu aplikacji.

Bezpieczeństwo - należy zaimplementować odpowiednie mechanizmy zabezpieczające, takie jak szyfrowanie haseł, uwierzytelnianie dwuskładnikowe, limity prób logowania, blokowanie konta w przypadku wielokrotnych nieudanych prób logowania, logowanie zdarzeń związanych z logowaniem, itp.

# 9. Warunki rozpoczęcia use case'u

1. Aplikacja jest uruchomiona: W celu rozpoczęcia procesu logowania do systemu, aplikacja musi być uruchomiona i dostępna dla użytkownika. Jeśli aplikacja jest wyłączona lub niedostępna, nie będzie możliwe rozpoczęcie procesu logowania.

2. Brak aktywnej sesji logowania: Jeśli nie istnieje aktywna sesja logowania, użytkownik będzie musiał rozpocząć proces logowania, aby uzyskać dostęp do chronionych zasobów systemu. Jeśli sesja logowania jest już aktywna, użytkownik może być przekierowany do ekranu powitalnego lub innej części aplikacji.

3. Aplikacja posiada mechanizmy logowania: Aby rozpocząć proces logowania, aplikacja musi posiadać odpowiednie mechanizmy logowania, takie jak formularze logowania, integracje z usługami uwierzytelniania zewnętrznego (np. OAuth, SAML) lub inne metody uwierzytelniania (np. biometryczne, jednorazowe kody).

4. Dostępność wymaganych zasobów: W przypadku procesu logowania, wymagane zasoby, takie jak serwer uwierzytelniania, baza danych z danymi użytkowników, odpowiednie połączenia sieciowe, muszą być dostępne i funkcjonalne, aby proces logowania mógł być rozpoczęty.

# 10. Stan końcowy

# Stan końcowy obejmuje dostęp użytkownika do chronionych zasobów i funkcji systemu, a także możliwość wylogowania się z aplikacji po zakończeniu sesji logowania.

# 11. Nierozwiązane problemy

1. Bezpieczeństwo hasła: Bezpieczeństwo hasła jest kluczowe w procesie logowania, jednak nadal wielu użytkowników stosuje słabe hasła lub używa tego samego hasła w wielu miejscach. Może to prowadzić do naruszenia bezpieczeństwa konta użytkownika w przypadku ataku hakerskiego lub kradzieży danych. Problemem może być również zabezpieczenie przesyłania hasła w procesie logowania, takie jak transmisja w formie tekstu czy brak używania bezpiecznych protokołów komunikacyjnych.

2. Zapomniane hasła: Użytkownicy często zapominają hasła, co może prowadzić do konieczności resetowania hasła lub odzyskiwania konta. Może to być problemem zarówno dla użytkowników, którzy nie pamiętają swojego hasła, jak i dla zespołu wsparcia technicznego, który musi obsługiwać te żądania resetowania hasła.

3. Nieautoryzowane logowanie: Nieautoryzowane logowanie to sytuacja, w której osoba nieuprawniona próbuje uzyskać dostęp do konta innego użytkownika. Może to występować na przykład w przypadku kradzieży danych logowania lub prób hakerskich. Zapobieżenie nieautoryzowanemu logowaniu może być wyzwaniem, zwłaszcza w przypadku złożonych ataków na bezpieczeństwo.

4. Audyt i monitorowanie: Audyt i monitorowanie logowania do aplikacji są istotne dla zapewnienia bezpieczeństwa. Jednakże, niektóre systemy mogą nie posiadać wystarczających mechanizmów audytu i monitorowania, co może prowadzić do trudności w identyfikowaniu nieautoryzowanego dostępu, prób ataków czy innych nieprawidłowości w procesie logowania.