

1. Nazwa use case'u

Logowanie do aplikacji

2. Wstęp (Opis ogólny)

Ten przypadek użycia (use case) opisuje proces, w którym użytkownik (np. klient lub sprzedawca) próbuje się zalogować do systemu. Celem tego jest potwierdzenie tożsamości użytkownika i umożliwienie mu korzystania z funkcji aplikacji. Use case jest częścią funkcjonalności bezpieczeństwa i kontroli dostępu w aplikacji.

3. Cel use case'u

Zapewnienie **bezpiecznego dostępu** do aplikacji wyłącznie dla **autoryzowanych użytkowników** (takich, którzy mają poprawny login i hasło). Jeśli dane są poprawne – użytkownik wchodzi do systemu. Jeśli nie – pojawia się komunikat o błędzie.

4. Lista aktorów (kto bierze udział)

- Klient
- Sprzedawca

5. Aktor inicjujący (kto zaczyna proces)

- Klient (np. osoba logująca się do aplikacji)

6. Uczestnicy

- Brak (żaden inny aktor nie bierze udziału w tym przypadku)

7. Przebieg podstawowy (główne kroki logowania)

Krok 1:

Użytkownik uruchamia aplikację i widzi formularz logowania.

Krok 2:

Użytkownik wpisuje **login i hasło** w odpowiednie pola formularza.

Krok 3:

Użytkownik klika przycisk „Zaloguj się”.

Krok 4:

System sprawdza, czy podane dane (login i hasło) są poprawne i istnieją w bazie danych.

Krok 5:

Jeśli dane są poprawne:

- System loguje użytkownika, przenosi go do strony głównej lub pulpitu aplikacji.
- System zapisuje w tle informację o sesji użytkownika (np. token logowania).

Krok 6:

Użytkownik widzi ekran główny aplikacji i może korzystać z funkcji systemu.

8. Wyjątki (co jeśli coś pójdzie źle)

Wyjątek 1: Niepoprawny login lub hasło

- Po kroku 4:
- System wyświetla komunikat: „Niepoprawny login lub hasło.”
- Użytkownik może spróbować ponownie.

Wyjątek 2: Brak połączenia z serwerem

- Po kroku 3:
- System pokazuje komunikat: „Brak połączenia z serwerem. Sprawdź połączenie internetowe.”

Wyjątek 3: Konto zablokowane (np. za dużo błędnych prób)

- Po kroku 4:
- System wyświetla: „Twoje konto zostało tymczasowo zablokowane. Spróbuj ponownie później.”

9. Przebiegi alternatywne

Alternatywny przebieg 1: Użytkownik nie ma konta

- Po kroku 1: użytkownik klika „Zarejestruj się”
- System przenosi go do formularza rejestracji nowego konta

10. Zagadnienia implementacyjne (na etapie wdrażania)

- System powinien **obsługiwać min. 100 jednoczesnych użytkowników** logujących się w tym samym czasie.
- **Bezpieczeństwo:** dane logowania muszą być przesyłane zaszyfrowanym protokołem (HTTPS).
- **Reakcja systemu:** odpowiedź na kliknięcie „Zaloguj się” powinna nastąpić **maksymalnie w 2 sekundy**.
- System powinien **logować nieudane próby logowania** do celów bezpieczeństwa.
- Użytkownik powinien być automatycznie **wylogowany po 30 minutach nieaktywności**.

11. Warunki rozpoczęcia use case’u

- Użytkownik **ma już konto** w aplikacji
- Aplikacja jest uruchomiona i działa
- Użytkownik **posiada login i hasło**
- Urządzenie ma **aktywny internet**

12. Stan końcowy (co się dzieje na końcu)

- Użytkownik jest **zalogowany** i ma dostęp do funkcji aplikacji
- System utworzył sesję użytkownika
- Użytkownik widzi ekran główny
- (W przypadku błędu: użytkownik pozostaje na stronie logowania)

13. nierozwiązane problemy / pytania do ustalenia

- Czy aplikacja będzie posiadać **logowanie dwuskładnikowe (2FA)**?
- Czy użytkownik może wybrać opcję „zapamiętaj mnie”?
- Jakie są zasady dotyczące **resetowania hasła**?
- Jak długo sesja pozostaje aktywna?
- Czy aplikacja ma **rejestrować miejsce logowania** (np. IP, lokalizacja)