Struktura use case

*Sklep internetowy - MegaKomp*

Wersja v11\_04\_2023

Data 11.04.2023

Spis treści

[1. Logowanie do aplikacji. 3](#_Toc131580315)

[2. Wstęp 3](#_Toc131580316)

[3. Cel use case'u 3](#_Toc131580317)

[4. Lista aktorów 3](#_Toc131580318)

[4.1 Aktor inicjujący 3](#_Toc131580319)

[4.2 Uczestnicy 3](#_Toc131580320)

[5. Przebieg use case'u 3](#_Toc131580321)

[6. Wyjątki 3](#_Toc131580322)

[7. Przebiegi alternatywne 4](#_Toc131580323)

[8. Zagadanienia implementacyjne 4](#_Toc131580324)

[9. Warunki rozpoczęcia use case'u 4](#_Toc131580325)

[10. Stan końcowy 4](#_Toc131580326)

[11. Nierozwiązane problemy 4](#_Toc131580327)

# 1. Logowanie do aplikacji.

Klient aplikacji loguje się do aplikacji.

# 2. Wstęp

Use case „Logowanie” opisuje proces logowania do systemu.

Klient jest aktorem, który uruchamia proces logowania do aplikacji.

System jest również aktorem, który wykonuje wiele czynności, takich jak wyświetlanie ekranu logowania, weryfikacja wprowadzonych danych logowania, przekierowywanie klienta do panelu głównego aplikacji itp.

Klient jest zależny od systemu w celu uzyskania dostępu do aplikacji. Bez zalogowania, klient nie może uzyskać dostępu do funkcji, które wymagają autoryzacji.

System jest zależny od klienta, aby wprowadził poprawne dane logowania. Bez poprawnych danych, system nie może uwierzytelnić tożsamości klienta.

# 3. Cel use case'u

Celem logowania jest potwierdzenie tożsamości klienta, aby zapewnić bezpieczeństwo i ochronę danych w systemie, oraz dokonanie zakupu towaru.

# 4. Lista aktorów

* Klient zarejestrowany (Klient)

## 4.1 Aktor inicjujący

Klient zarejestrowany (Klient)

# 5. Przebieg use case'u

Krok 1.

Klient naciska przycisk „Zaloguj” na stronie głównej, aby wyświetlić stronę z logowaniem do aplikacji.

Krok 2.

System wyświetla stronę z formularzem logowania z polami na adres e-mail i hasło.

Krok 3.

Klient wprowadza swój adres e-mail i hasło.

Krok 4.

Klient naciska przycisk „Zaloguj się”.

Krok 5.

System przeprowadza autoryzację. //weryfikuje adres e-mail i hasło.

Krok 6.

System informuje klienta o zalogowaniu i przekierowuje klienta do strony z artykułami.

Krok 7.

Klient może korzystać z aplikacji.

# 6. Wyjątki

# <Wyjątek 1>

Klient podał nieprawidłowy e-mail i hasło, o czym jest informowany pojawiającym się komunikatem. Klient powinien wprowadzić ponownie e-mail i hasło.

# <Wyjątek 2>

Wystąpił problem po stronie serwera, system przekazuje informacje o błędzie serwera. Na stronie wyświetla się informacja „Server-error”, oraz postępowanie w celu wyeliminowania błędu.

# 7. Przebiegi alternatywne

# <Przebieg Alternatywny 1>

Krok 3

Klient wprowadza swój adres e-mail i hasło.

Krok 4

Klient rezygnuje z procesu logowania, np. przechodząc do strony głównej. System przechodzi do stanu sprzed próby logowania.

# <Przebieg Alternatywny 2>

Krok 5

System nie przeprowadza autoryzacji.

Krok 6

System nie potwierdził klienta, wyświetla komunikat o błędzie i prosi o ponowne podanie e-maila oraz hasła.

# 8. Zagadnienia implementacyjne

Bezpieczeństwo – implementacja odpowiednich mechanizmów zabezpieczających np. blokowanie konta w przypadku wielokrotnych nieudanych prób logowania.

Weryfikacja danych logowania - system musi zweryfikować, czy wprowadzone przez klienta 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 klienta.

# 9. Warunki rozpoczęcia use case'u

Aplikacja wymaga autoryzacji - warunkiem rozpoczęcia procesu logowania jest próba dostępu do funkcjonalności, która wymaga autoryzacji, np. dostęp do chronionego obszaru aplikacji lub do informacji tylko dla zalogowanych klientów.

Zmiana danych logowania - jeśli klient chce zmienić swoje dane logowania, na przykład zmienić hasło lub nazwę klienta, konieczne jest zalogowanie się ponownie, aby potwierdzić swoją tożsamość.

Nowy klient - jeśli klient nie posiada jeszcze konta w systemie, konieczne jest utworzenie nowego konta poprzez proces rejestracji, który wymaga potwierdzenia tożsamości.

Przeglądanie historii działań - jeśli klient chce przeglądać historię swoich działań w systemie, może to wymagać autoryzacji, a więc konieczne jest rozpoczęcie procesu logowania.

# 10. Stan końcowy

Klient zostaje zalogowany poprawnie i pojawia się informacja w prawym górnym rogu o zalogowaniu oraz ma dostęp do chronionych funkcjonalności systemu.

Klient podał błędne dane logowania i nie zostaje zalogowany.

Klient anuluje proces logowania i powraca do stanu przed próbą logowania.

Klient zostaje wylogowany z systemu i traci dostęp do chronionych funkcjonalności.

# 11. Nierozwiązane problemy

[Nie dotyczy]