Opis systemu ASSASSIN

Tomasz Chady

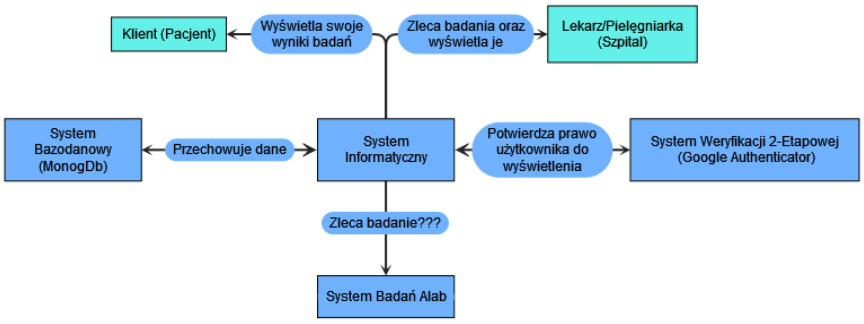
January 22, 2024

1 Wprowadzenie

ASSASSIN to system do przechowywania i udostępniania wyników badań pacjentom i personelowi medycznemu. System jest przeznaczony dla szpitali, klinik i laboratoriów. Głównym celem systemu jest zapewnienie bezpiecznego dostępu do wyników badań. System jest dostępny poprzez aplikację mobilną oraz stronę internetową. Dzięki zaimplementowaniu standardowych informatycznych rozwiązań system jest o wiele bezpieczniejszy i zapewnia większy poziom prywatności niż tradycyjne rozwiązania.

2 Zakres systemu

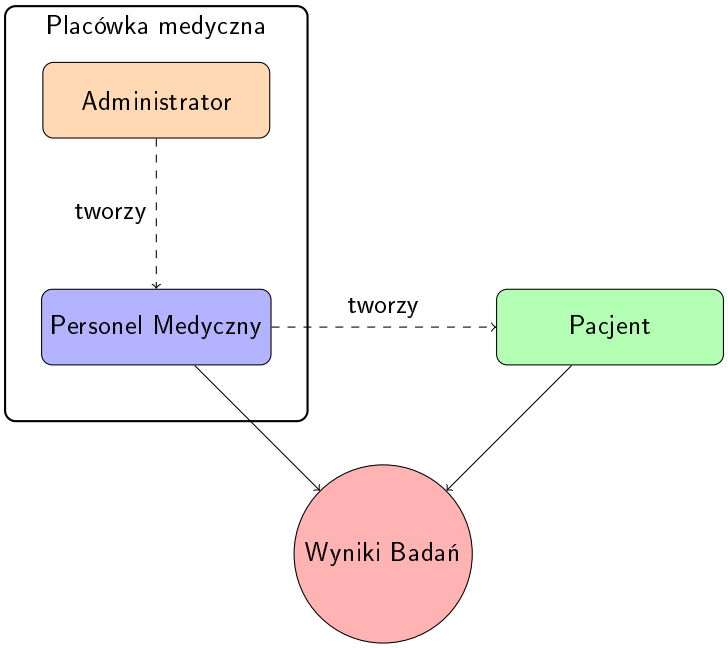
System umożliwia przechowywanie wyników badań pacjentów. Wyniki badań są dostępne dla personelu medycznego oraz pacjentów. Personel medyczny może dodawać wyniki badań do systemu. Pacjenci mogą przeglądać wyniki swoich badań zdalnie przez internet. Wyniki badań są dostępne poprzez aplikację mobilną oraz stronę internetową i są dostępne tylko dla uprawnionych osób. Dodatkowo system umożliwia odebranie wyników badań fizycznie w placówce medycznej. Ogólny schemat systemu jest przedstawiony na schemacie 1.



Schemat 1: Schemat systemu ASSASSIN

3 Role użytkowników

System posiada trzy role użytkowników: pacjent, personel medyczny oraz administrator. Każda rola definiuje co użytkownik może robić w systemie. Poniżej przedstawiono szczegółowy opis każdej z ról, a na schemacie 2 przedstawiono graficznie relacje między rolami.



Schemat 2: Schemat ról w systemie ASSASSIN

3.1 Pacjent

Konto pacjenta jest tworzone przez personel medyczny podczas pierwszego kontaktu z pacjentem. Pacjent identyfikowany jest poprzez anonimowy login, hasło oraz aplikację 2FA. W ten sposób minimalizowane jest ryzyko wycieku danych osobowych pacjenta poprzez błąd użytkownika. Pacjent może przeglądać wyniki swoich badań oraz odbierać wyniki badań fizycznie w placówce medycznej. Ewentualne przejęcie konta pacjenta przez osobę trzecią nie powinno spowodować katastrofalnego wycieku danych osobowych, albowiem system minimalizuje ilość przechowywanych danych. Dobrze to wpływa na koszty utrzymania systemu oraz na bezpieczeństwo użytkowników.

3.2 Personel Medyczny

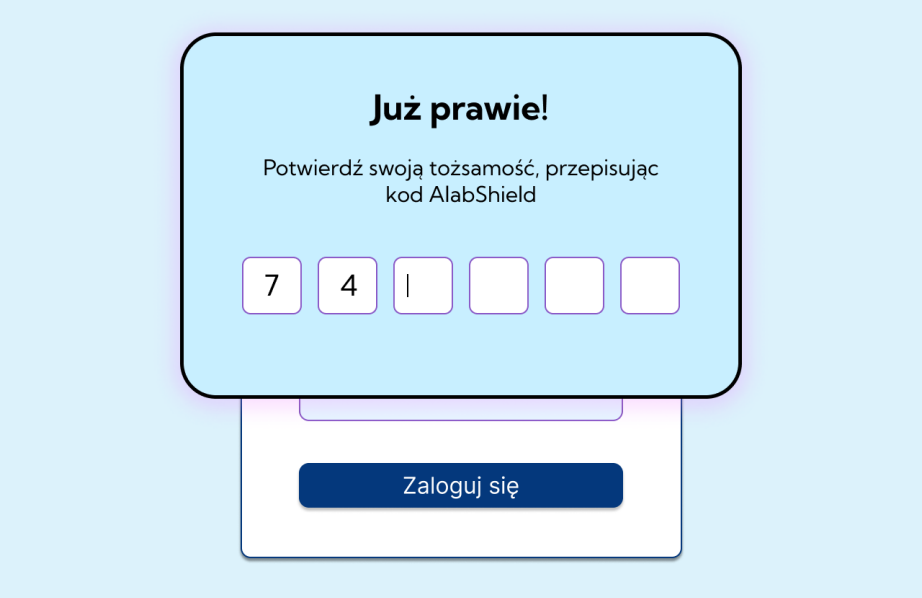
Konto personelu medycznego jest tworzone przez administratora. Jest ono powiązane z konkretną placówką medyczną oraz konkretnym nazwiskiem. Autoryzacja personelu medycznego następuje poprzez placówkę medyczną. Personel medyczny może dodawać wyniki badań do systemu oraz przeglądać wyniki badań pacjentów swojej placówki medycznej. Dostęp do konta personelu medycznego jest możliwy tylko z poziomu sieci wewnętrznej placówki medycznej. W ten sposób minimalizowane jest ryzyko wycieku danych osobowych pacjentów poprzez błąd użytkownika. Ewentualne przejęcie konta personelu medycznego jest praktycznie niemożliwe poprzez wymóg bycia fizycznie w placówce medycznej.

3.3 Administrator

Konto administratora jest tworzone podczas instalacji systemu. Administrator może tworzyć konta personelu medycznego oraz zarządzać placówkami medycznymi. Administrator nie ma dostępu do wyników badań pacjentów.

4 Bezpieczeństwo

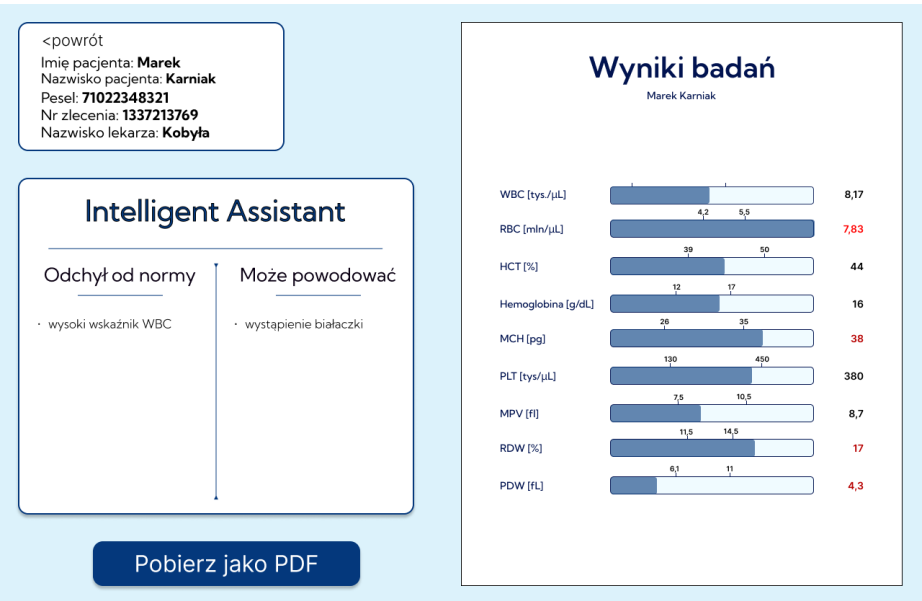
Bezpieczeństwo systemu oraz przechowywanych danych było priorytetem podczas projektowania systemu. Poprzez zastosowanie 2FA oraz anonimowych loginów minimalizowane jest ryzyko wycieku danych osobowych pacjentów poprzez błąd użytkownika. Konta personelu medycznego są zabezpieczone poprzez blokadę zdalnego logowania i w ten sposób włamanie się na konto personelu jest znacznie utrudnione. Przykładowy widok weryfikacji dwu stopniowej jest przedstawiony na schemacie 3.



Schemat 3: Widok weryfikacji dwu stopniowej

5 Dostęp do badań

Badania są dostępne poprzez aplikację mobilną oraz stronę internetową w postaci wirtualnej. Można też na podstawie badań wygenerować i pobrać z systemu pdf. Wyniki badań są dostępne tylko dla uprawnionych osób. Widok pobierania wyników jest przedstawiony na schemacie 4.



Schemat 4: Widok pobierania wyników