Bezpieczeństwo połączenia legitymacja-backend

Cel

Celem bezpieczeństwa połączenia legitymacja-backend jest zaszyfrowanie i uwierzytelnienie danych wysyłanych z lodówek na backend w bibliotechu D-21.

Rozwiązania

* legiymacja i backend połączone są przez protokół HTTPS.
* interfejs ISO 7816-2,3
* Przesyłane dane są podpisywanie przez każdą legitymację za pomocą podpisu cyfrowego. Każda lodówka ma unikalny klucz prywatny, a baza kluczy publicznych znajduje się po stronie backendu. Kiedy legitymacja przygotowuje treść zapytania, podpisuje ją swoim kluczem, a następnie wysyła na serwer. Serwer na podstawie id legitymacji, sprawdza czy ta legitymacja rzeczywiście podpisała zapytanie.

Zabezpieczenia połączenia frontend-backend

Cel

Celem bezpieczeństwa połączenia frontend backend jest ochrona danych użytkownika oraz uwierzytelnienie jego połączenia z aplikacją.

Rozwiązania

* Frontend i backend połączone są za pomocą protokoły HTTPS.
* Z każdą legitymacją połączone jest konto ze z góry określonym usernamem i hasłem.
* Użytkownik po pierwszym zalogowaniu powinien zmienić username i hasło oraz podać swój adres email.
* Hasło użytkownika jest przechowywane zahashowane w bazie danych.
* Połączenie z bazą danych jest lokalne; nie ma możliwości połączenia się z nią z zewnątrz.
* Uwierzytelnienie użytkownika następuje po sprawdzeniu czy hasło jest prawidłowe. Frontend wysyła na backend hasło plaintextem, a serwer porównuje z bazą danych czy jest ono prawidłowe.
* Użytkownik pozostaje zalogowany w aplikacji dzięki tokenom sesji.
* Po wysłaniu prośby o zmianę danych logowania, użytkownik otrzymuje email z jednorazowym linkiem za pomocą którego może zmienić te dane w ciągu następnych 10 minut.