Pełnomocnik ds. Rozwoju i Informatyzacji
Naczelnej Izby Lekarskiej

lek. Piotr Kalkowski

Naczelna Izba Lekarska –19.05.2023

Parametry techniczne systemu do głosowania

Dokument opracowany na zlecenie Krajowej Komisji Wyborczej

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

SPIS TREŚCI

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

1 WPROWADZENIE

1.1 CEL DOKUMENTU

Dokument opisuje koncepcję realizacji technicznej Systemu do Głosowania na potrzeby Naczelnej Izby Lekarskiej oraz Okręgowych Izb Lekarskich. W dokumencie zdefiniowana została wysokopoziomowa architektura proponowanego rozwiązania, zarekomendowany został tzw. stos technologiczny do realizacji projektu, opisane zostały funkcjonalności systemu do głosowania i sposób ich realizacji.

1.2 CEL BIZNESOWY PROJEKTU

Celem biznesowym projektu ma być możliwość przeprowadzania wyborów zgodnie z regulacjami prawnymi dot. funkcjonowania Izb Lekarskich w Polsce, który umożliwi głosowanie w trybie online z poszanowaniem podstawowych cech głosowania (tajność, demokratyczność, wiarygodność).

Integralną częścią procesu głosowania, obsługiwaną w projektowanym systemie jest zarządzanie: przypisaniem lekarzy do rejonów wyborczych, ewidencja kandydatów, tworzenie rejonów wyborczych.

1.3 CZAS REALIZACJI

Planowany termin wydania wersji RC to koniec 4 kwartału 2023 r., zaś z początkiem III kwartału 2023 r. oczekiwany jest wstępnie funkcjonalny back-end, a z jego końcem wersja beta front-end'u. W I kwartale 2024 r. planowane są testy wersji RC, a pod koniec wydanie wersji finalnej.

2 GŁÓWNE ZAŁOŻENIA PROJEKTOWE

2.1 SPOSÓB DZIAŁANIA

Głosowanie 'online' + Głosowanie listowne

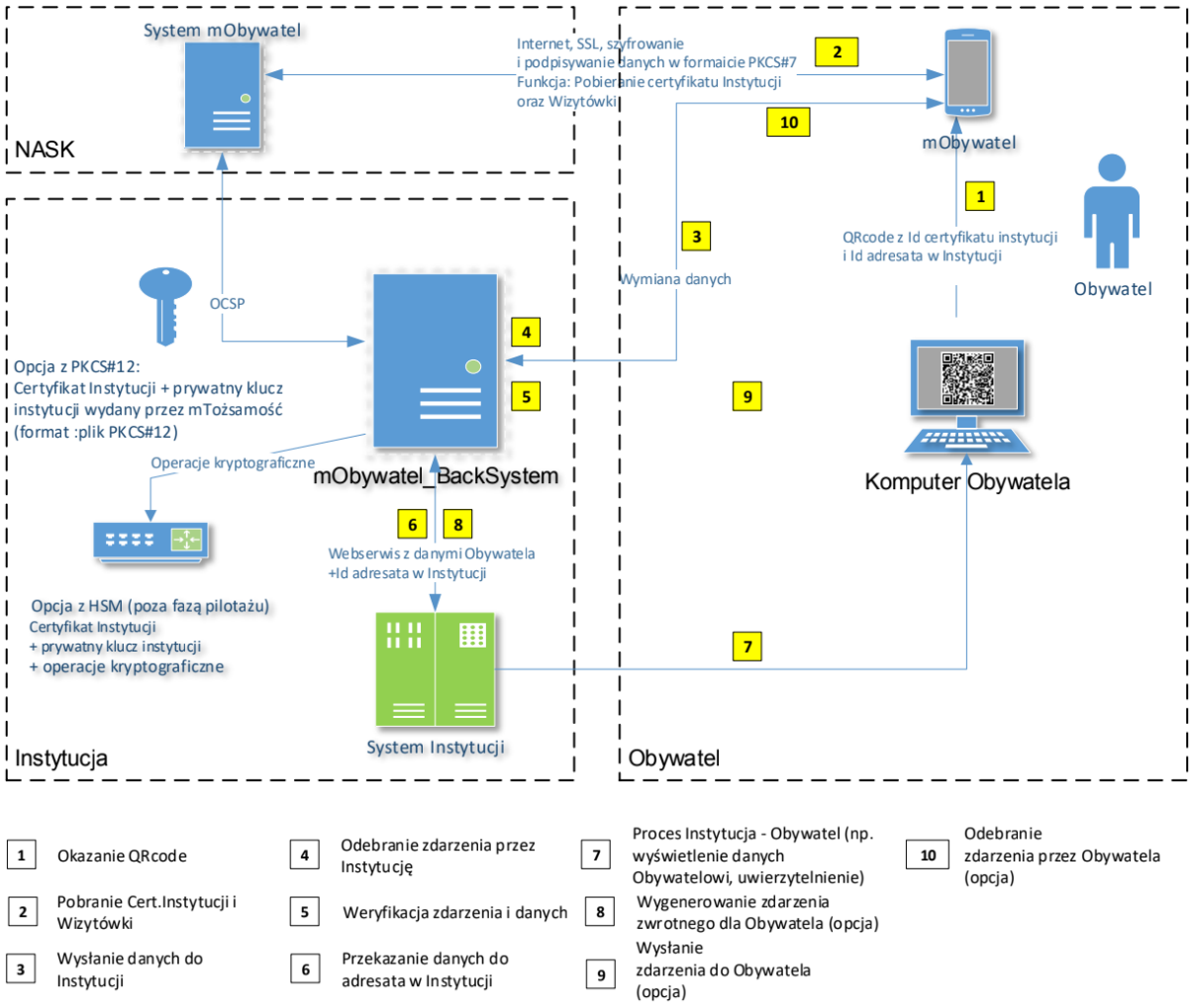
- W przypadku oddania dwóch głosów, priorytet ma głos online
- Głosy listowne będą podliczane po zakończeniu głosowania online, zbiorcze wyniki z głosowania listownego zostaną wprowadzone do systemu i dopiero wówczas nastąpi publikacja ostatecznych wyników
- Zgłoszenia kandydatur realizowane będą w formie hybrydowej

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

Uwierzytelnienie z wykorzystaniem aplikacji mObywatel



Główne zasady głosowań:

- Głosujący dysponuje liczbą głosów wynikającą z rozmiaru rejonu (algorytm zostanie przekazany przez NIL)
- Głosy wszystkich są równe
- Oddany głos jest głosem ostatecznym

2.2 ZAŁOŻENIA TECHNICZNE

Zarządzanie uprawnieniami realizowane z poziomu AD

2.3 CYKL ŻYCIA GŁOSOWAŃ

FAZA ZAPLANOWANEGO GŁOSOWANIA

Moment wejścia w fazę: zdefiniowanie głosowania przez administratora

Aktywne funkcjonalności:

- Możliwość przechodzenia lekarzy pomiędzy OIL
- Możliwość zmiany rejonów wyborczych

FAZA ZGŁASZANIA KANDYDATUR

Moment wejścia w fazę: z datą ustaloną przez administratora ORAZ po zatwierdzeniu przez Komisję Wyborczą sygnaturą uchwały

Aktywne funkcjonalności:

- Od tej fazy, zmiany OIL lekarza nie mają wpływu na okręg głosowania
- Pobranie listy lekarzy do systemu głosowania
- Możliwość zgłaszania kandydatur -> wprowadzanie zgłoszeń do systemu

FAZA GŁOSOWANIA ONLINE

Moment wejścia w fazę: z datą ustaloną przez administratora ORAZ po zatwierdzeniu przez **właściwą** Komisję Wyborczą sygnaturą uchwały

Aktywne funkcjonalności:

- Od tej fazy, brak możliwości zmiany rejonu wyborczego
- Możliwość oddawania głosów

FAZA PO GŁOSOWANIU ONLINE

Moment wejścia w fazę: z datą ustaloną przez administratora (datą zakończenia głosowania online) ORAZ po zatwierdzeniu przez właściwą KW sygnaturą uchwały

Aktywne funkcjonalności:

- Od tej fazy, brak możliwości głosowania

- Następuje zliczenie głosów listownych, wprowadzenie zagregowanych wyników listownych do systemu
- Wygenerowanie wyników (online+listowne)

2.4 ATRYBUTY GŁOSOWANIA I SPOSÓB ICH ZAGWARANTOWANIA

Cecha	Opis	Krytyczność
Wiarygodność	1. Złożonego głosu nie można zmienić 2. Nieprawidłowy głos nie może zostać policzony 3. Wyborca ma pewność że jego głos został oddany poprawnie	**WYMAGANE** **WYMAGANE** **WYMAGANE**
Demokratyczność	4. Tylko osoby uprawnione do głosowania mogą głosować 5. Każda osoba może oddać jeden głos	**WYMAGANE** **WYMAGANE**
Tajność	6. Nikt nie może powiązać głosu z wyborcą	**WYMAGANE**
Weryfikowalność	7. Przechowywanie informacji o tym kto oddał głos kanałem online. Głosujący może zweryfikować, że jego głos został oddany 8. Wyborca po oddaniu głosu może zweryfikować na kogo został oddany jego głos	**WYMAGANE** **KASACJA**
Odporność	9. W przypadku nie oddania głosu przez wyborcę, żadna ze stron nie może oddać głosu w jego imieniu	**KASACJA**

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

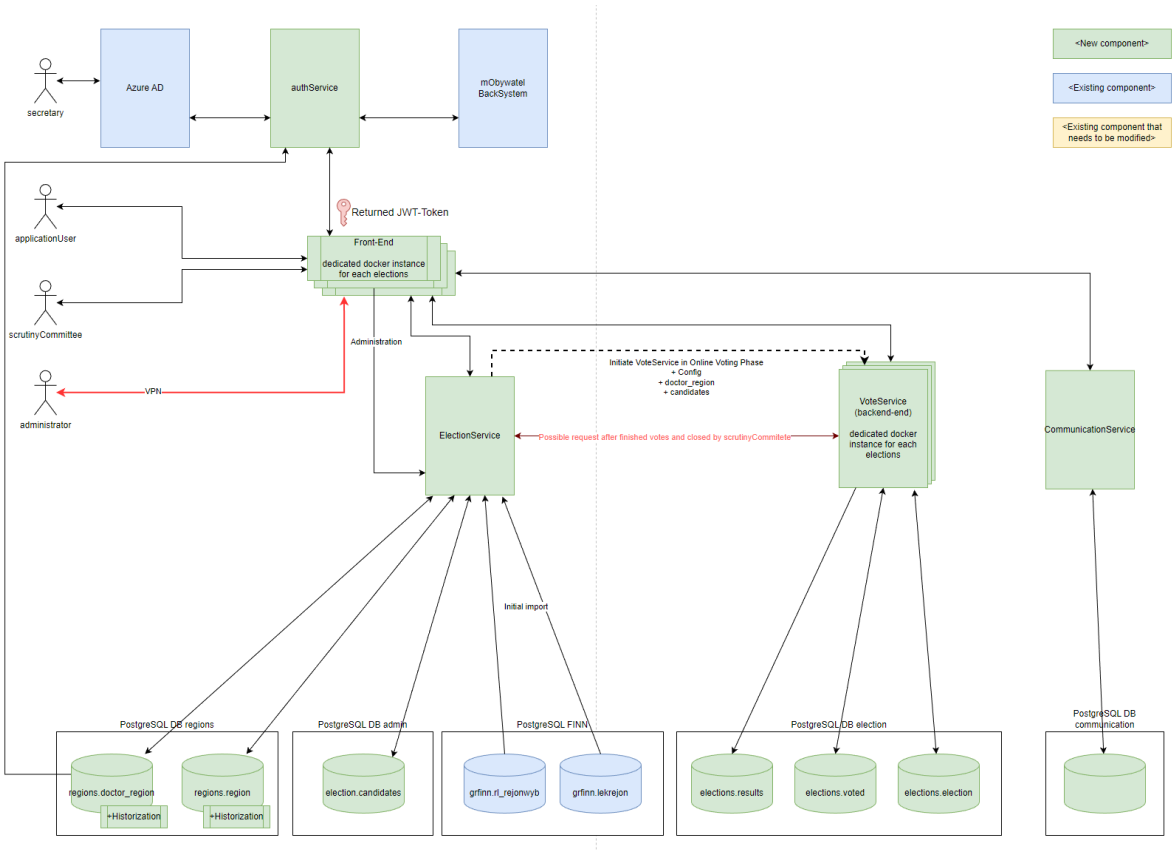
3 ARCHITEKTURA WYSOKOPOZIOMOWA

3.1 TECHNOLOGIE DO ZASTOSOWANIA W PROJEKCIE

Wybór wersji ze względu na najnowszy release na dzień pisania niniejszego dokumentu.

Technologia	Wersja	Zastosowanie w projekcie
Java	17 (Open Source)	**Główny język programowania po stronie backendu aplikacji we wszystkich mikroserwisach. Jest to język kompilowany.**
SpringBoot	3	**Najpopularniejszy framework języka Java służący przyspieszeniu developmentu oraz zwiększający bezpieczeństwo aplikacji.**
PostgreSQL	15	**Relacyjna baza danych wykorzystana w celu trwałego zapisywania danych.**
Angular	15/16	**Jeden z najpopularniejszych frameworków języka javascript/typescript obsługujący funkcjonalność aplikacji widoczną dla użytkownika.**
Docker	23	**Narzędzie służące wirtualizacji środowiska. Umożliwia łatwe zarządzanie wieloma serwisami na jednej maszynie fizycznej (serwerze).**

3.2 DIAGRAM ARCHITEKTURY

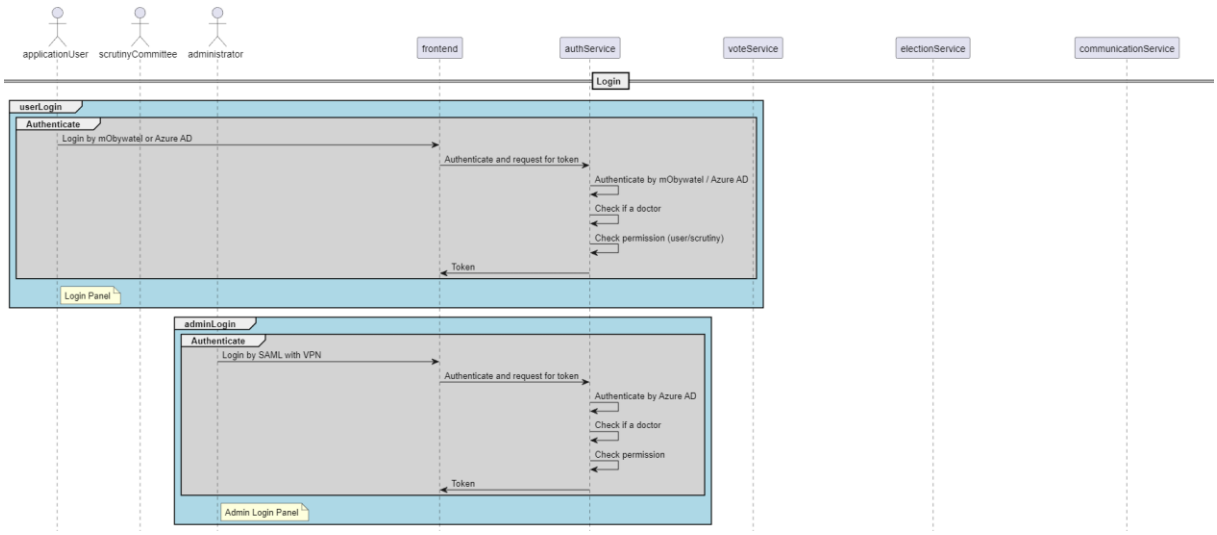


Lista komponentów:

Technologia	Typ	Zastosowanie w projekcie
BackSystem	**Istniejący komponent** Microservice BackEnd	**Serwis dostarczony przez mObywatel. Służy do komunikacji z mObywatelAPI.**
mObywatelAuthService	Microservice BackEnd	**Mikroserwis przeprowadzający proces autoryzacji z wykorzystaniem serwisu BackSystem oraz uwierzytelnienia z wykorzystaniem bazy danych.**
ElectionService	Microservice BackEnd	**Mikroserwis odpowiedzialny za zarządzanie głosowaniami w sposób administracyjny, jak również przez komisję skrutacyjną.**
VoteService	Microservice BackEnd	**Mikroserwis odpowiedzialny za przeprowadzenie głosowania.**
CommunicationService	Microservice BackEnd	**Mikroserwis pozwalający na komunikację użytkowników z administratorami aplikacji.**
Aplikacja frontendowa	FrontEnd	**Aplikacja umożliwiająca użytkownikowi pracę w systemie.**
Baza Systemu do Głosowań	DB PSQL	
Baza FINN	**Istniejący komponent** DB PSQL	

3.3 DIAGRAM SEKWENCJI DLA POSZCZEGÓLNYCH OPERACJI

3.3.1 LOGOWANIE

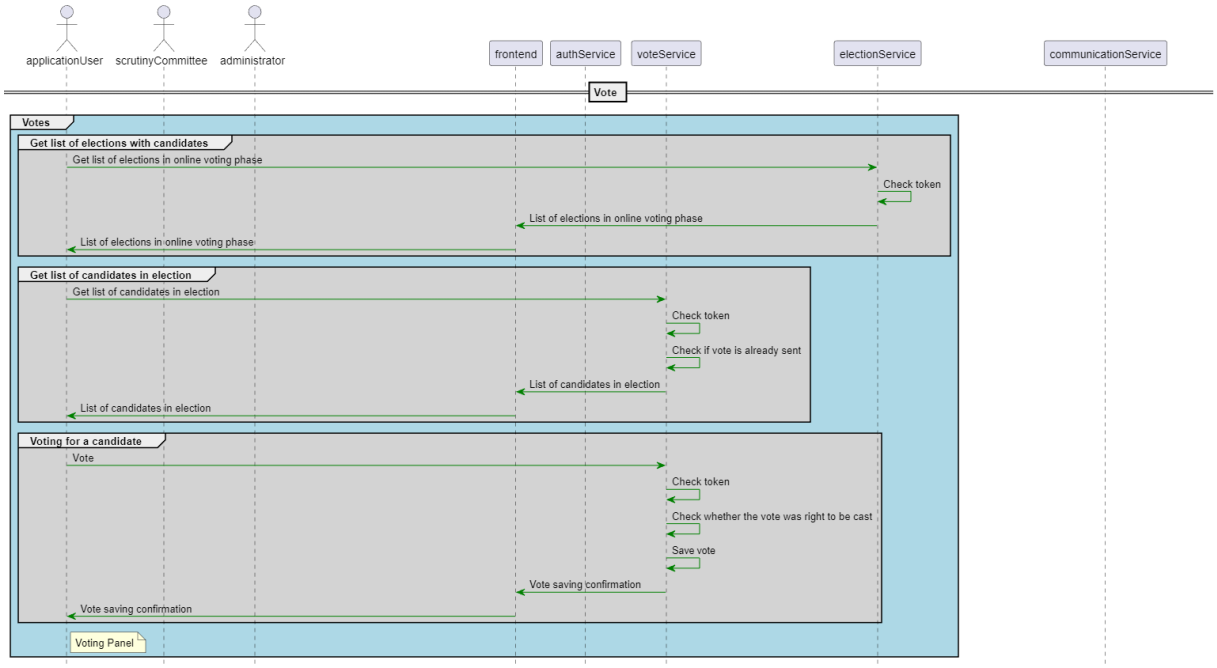


Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

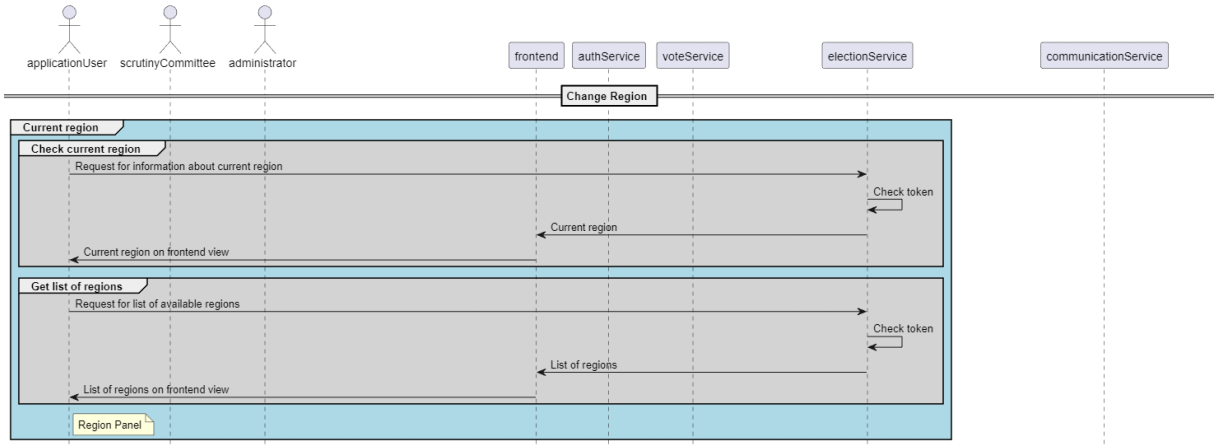
e-mail: piotr.kalkowski@nil.org.pl

3.3.2 GŁOSOWANIE



3.3.3 ZMIANA REGIONU

3.3.3.1 OBECNY REGION

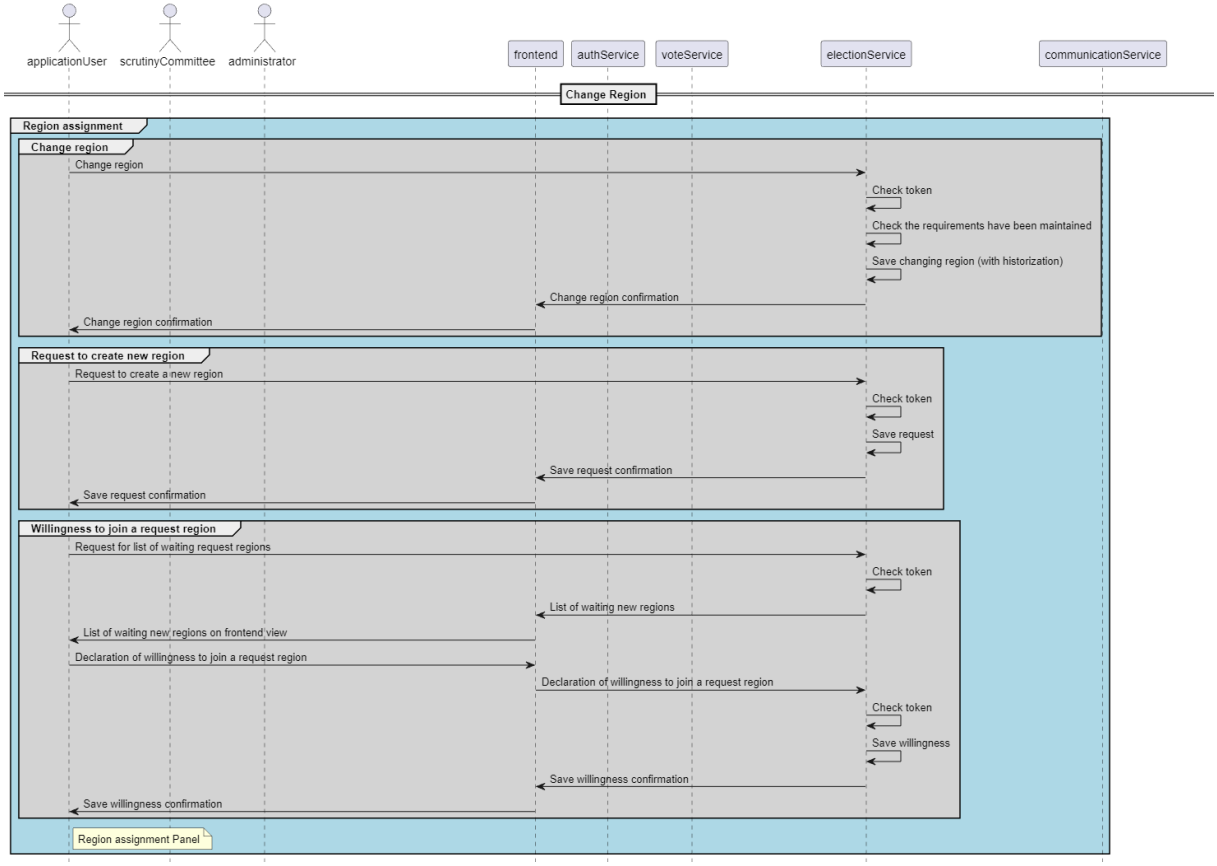


3.3.3.2 PRZYDZIAŁ REGIONU

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl



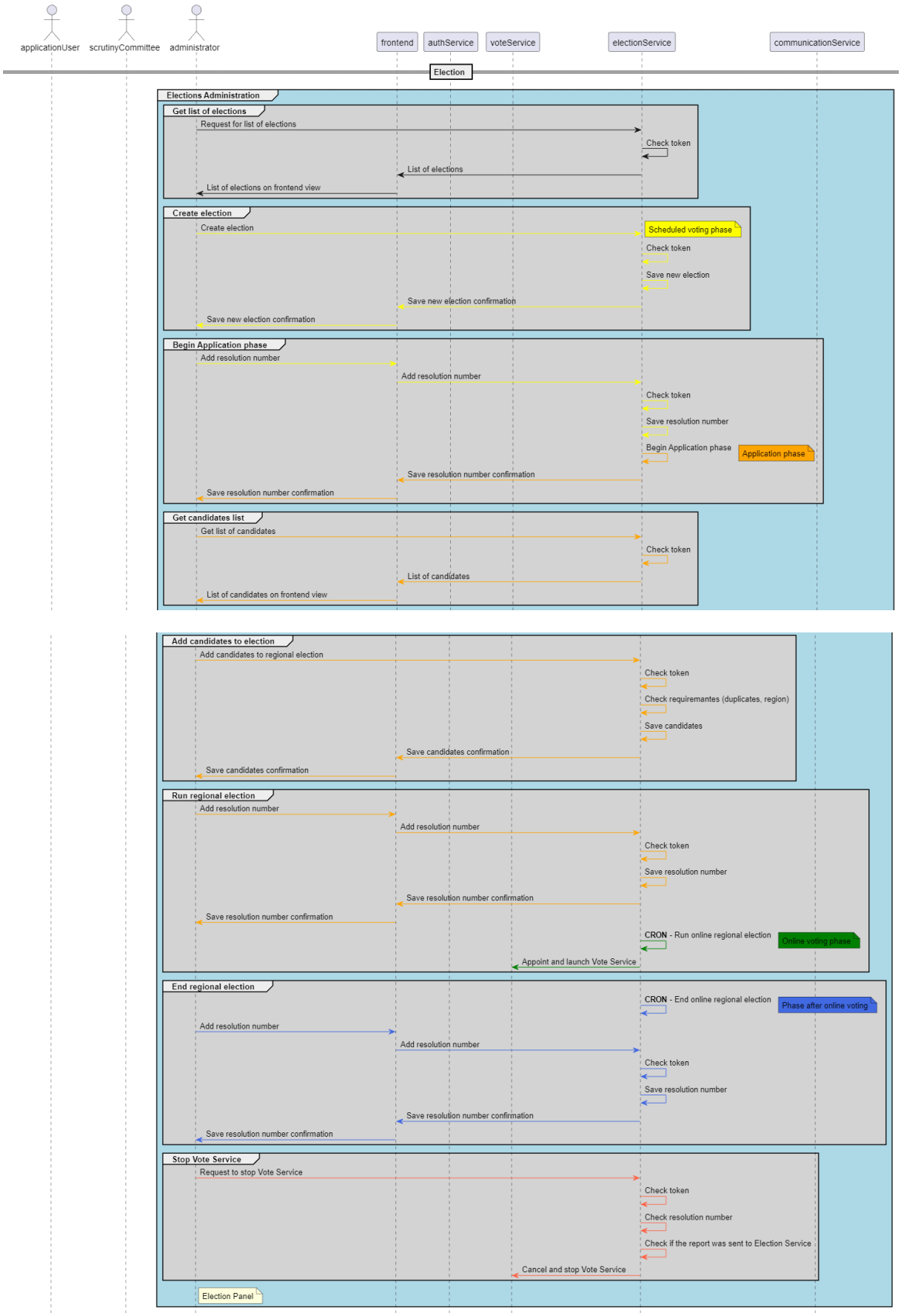
3.3.4 WYBORY

Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

3.3.4.1 ADMINISTRACJA WYBORAMI

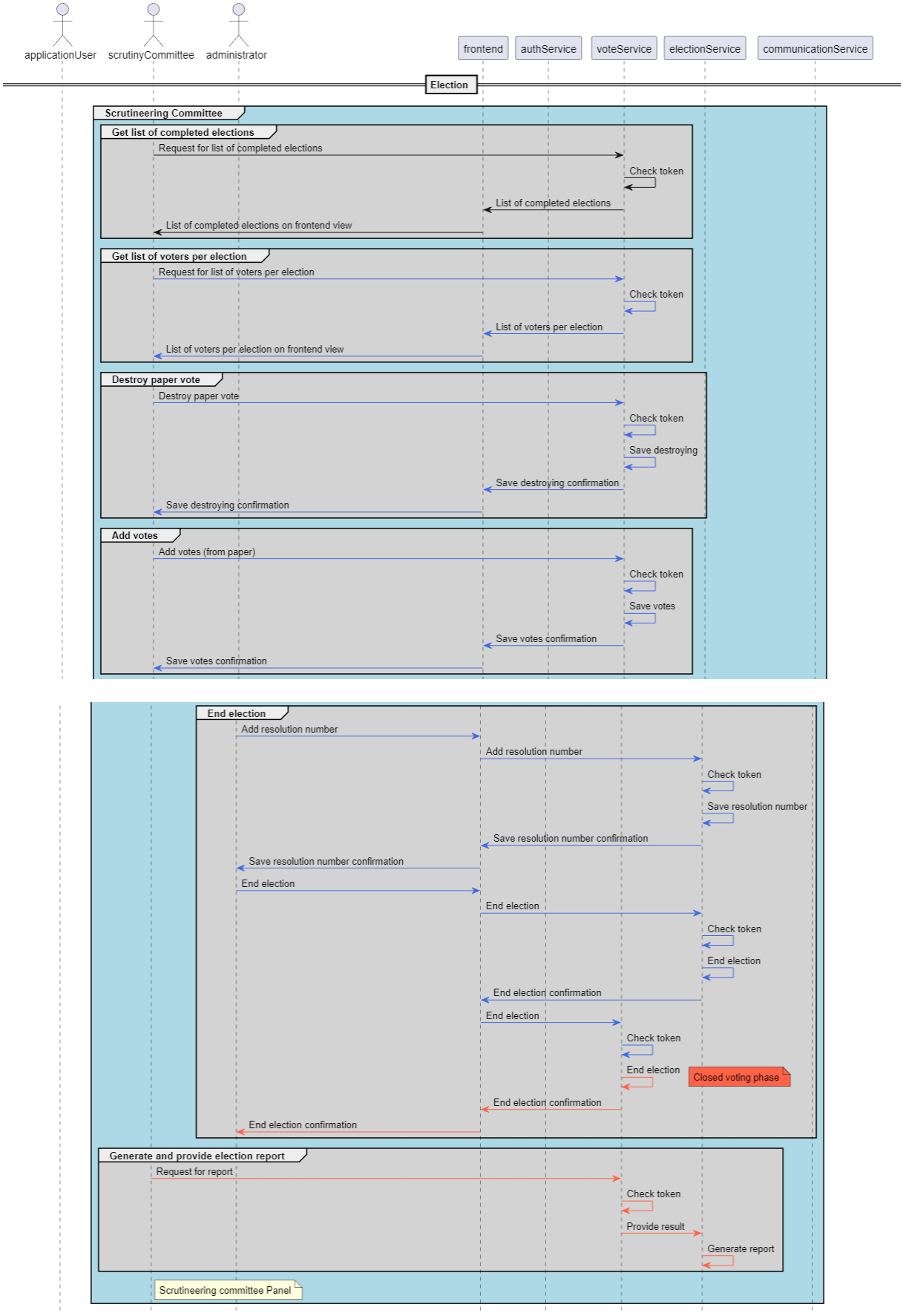


Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

3.3.4.2 KOMISJA SKRUTACYJNA



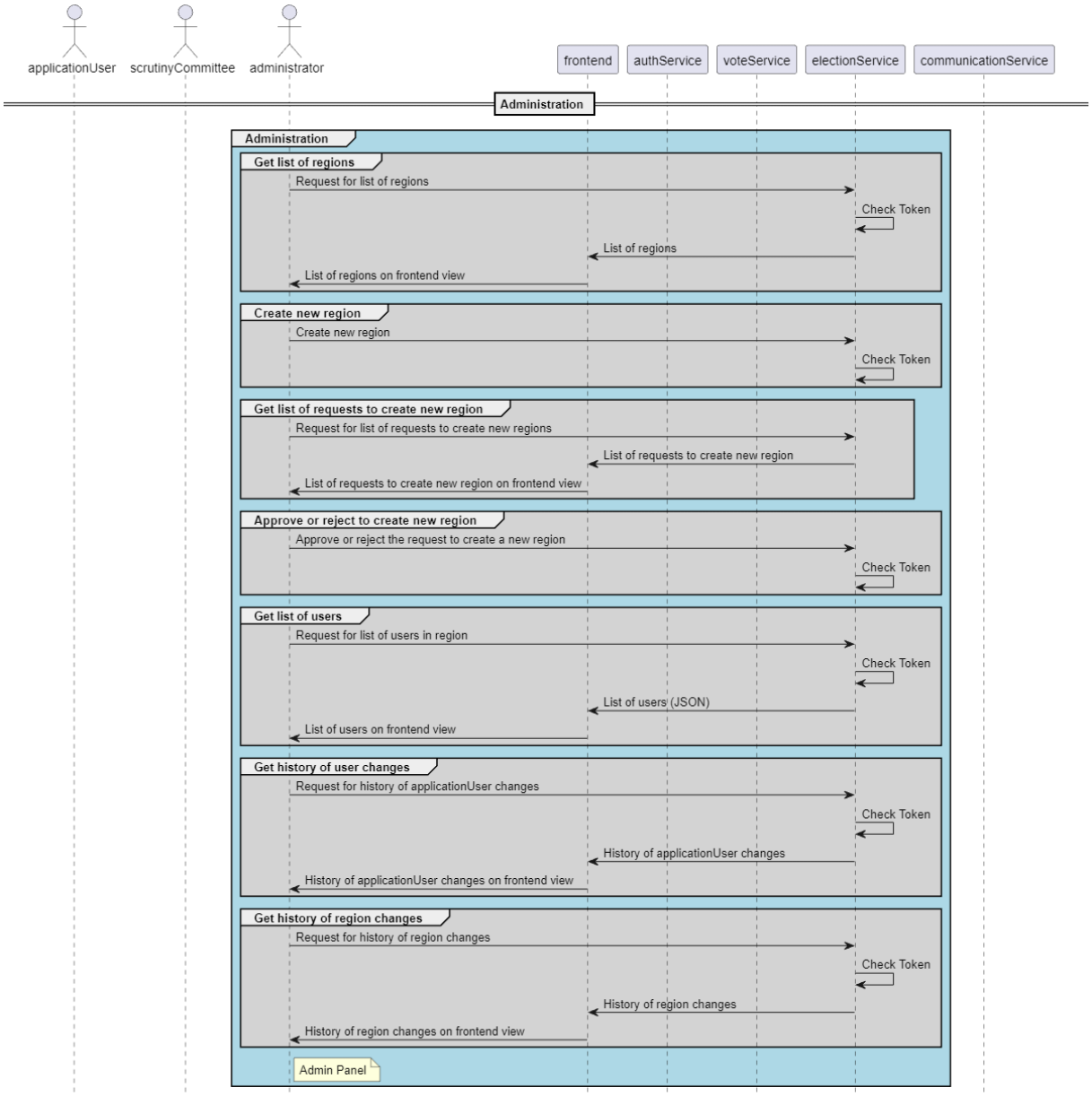
Naczelna Izba Lekarska, ul. Jana Sobieskiego 110, 00-764 Warszawa

tel. +48 501 134 793

e-mail: piotr.kalkowski@nil.org.pl

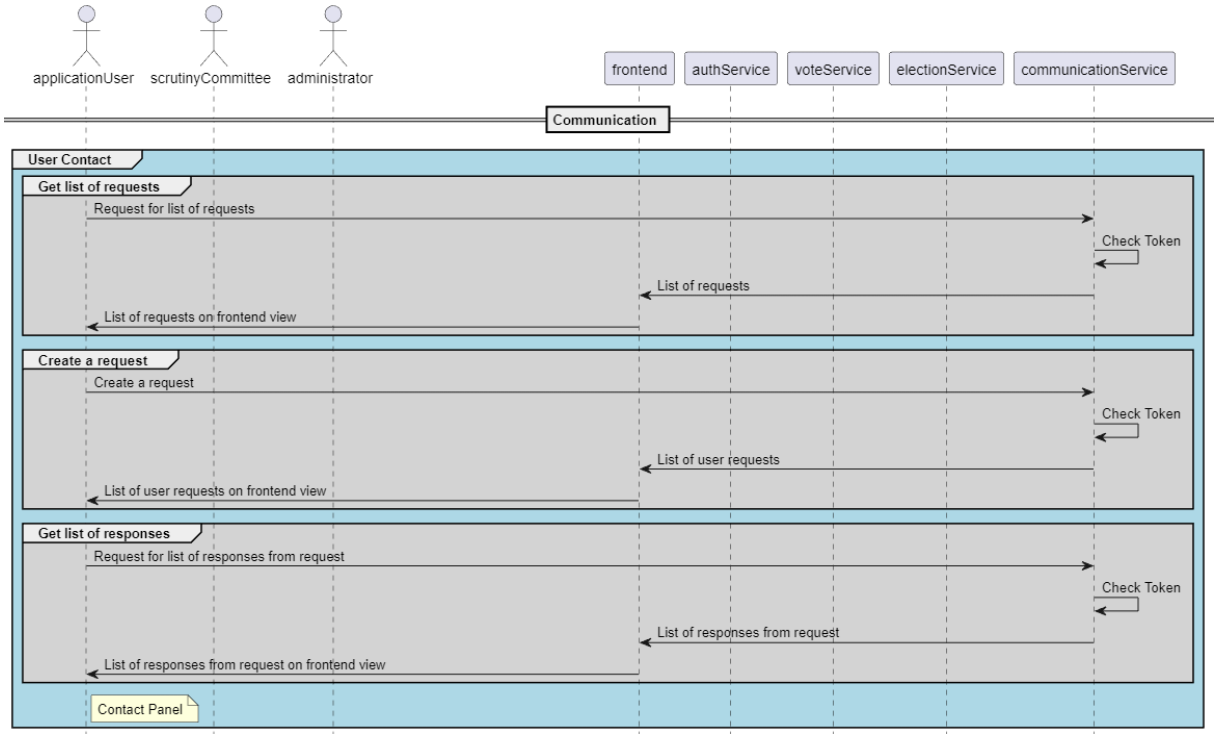
*możliwym rozwiązaniem byłoby zastąpienie drogi „Get list of voters per election” drogą „Check if voted per election” w celu minimalizacji informacji przekazywanych komisji skrutacyjnej.

3.3.5 ADMINISTRACJA

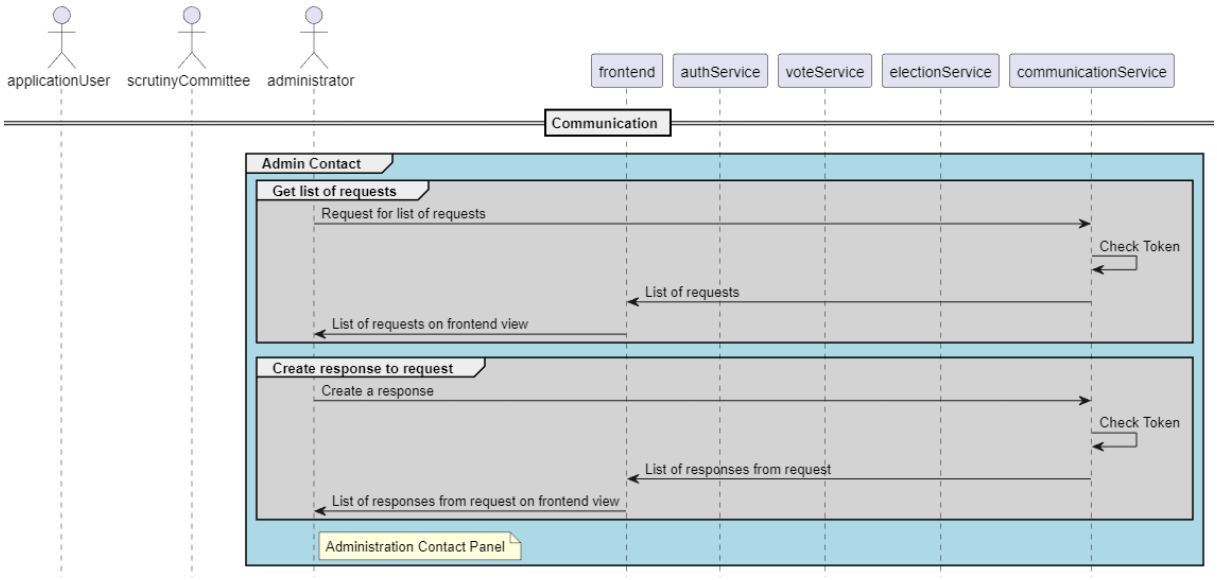


3.3.6 KOMUNIKACJA

3.3.6.1 KOMUNIKACJA UŻYTKOWNIKA

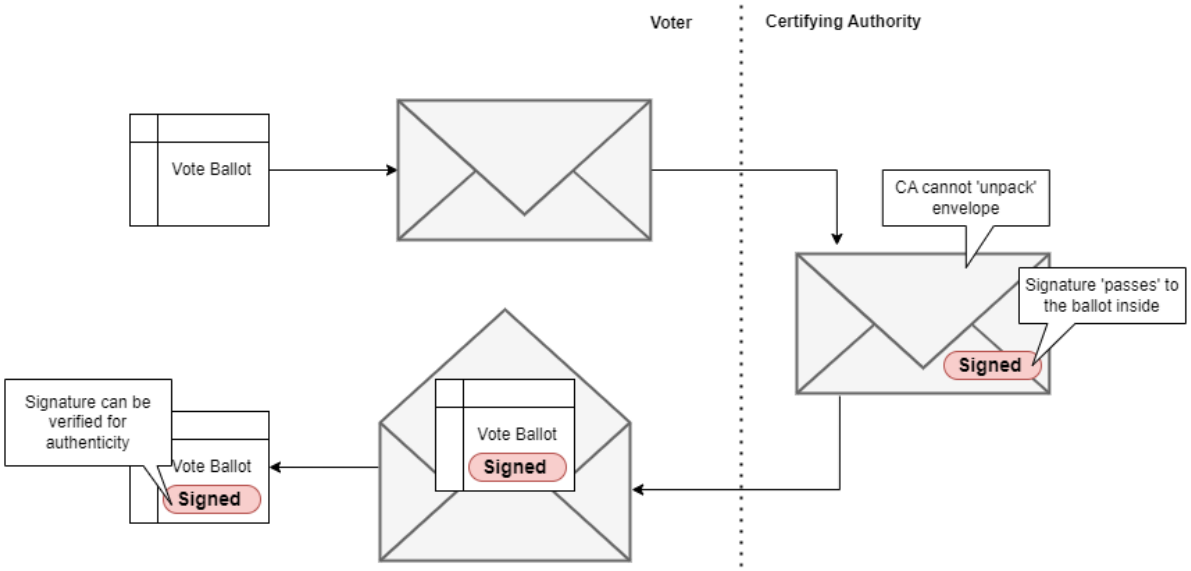


3.3.6.2 KOMUNIKACJA ADMINISTRATORA

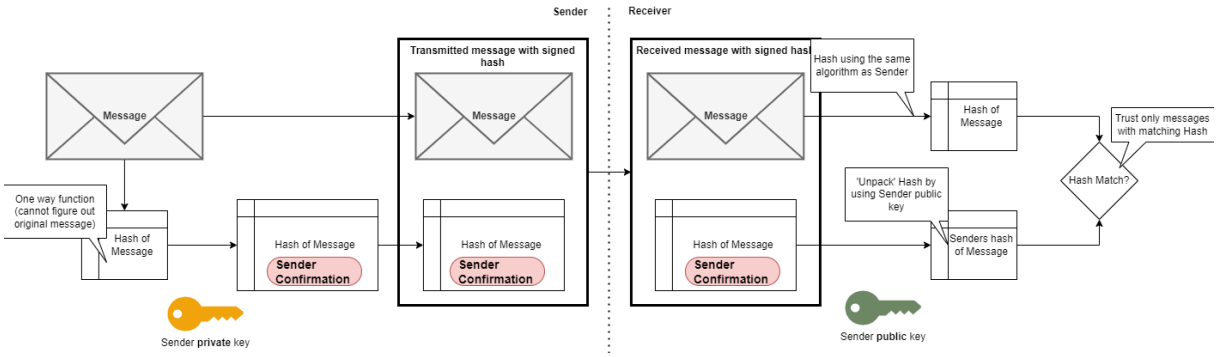


4 APPENDIX A: MECHANIZMY KRYPTOGRAFICZNE DO IMPLEMENTACJI PROTOKOŁU GŁOSOWANIA

TZW. ŚLEPY PODPIS



INTEGRALNOŚĆ WIADOMOŚCI POPRZEZ PRZEKAZYWANIE PODPISANEGO HASH WIADOMOŚCI W KOMUNIKACIE



SZYFROWANIE KLUCZEM ASYMETRYCZNYM

Nadawca przed wysłaniem wiadomości szyfruje zawartość kluczem publicznym Odbiorcy. Dzięki temu tylko odbiorca jest w stanie odszyfrować wiadomość (z wykorzystaniem własnego klucza prywatnego).