



UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
NOVI SAD



Grupa 16.

Nikola Dragaš , PR83/2015

Nemanja Zilić , PR91/2015

Ilija Hornjak , PR92/2015

Milan Đokić , PR105/2015

Zadatak 22.

Sigurnost i bezbednost u elektroenergetskim sistemima
- Primenjeno softversko inženjerstvo -

Novi Sad, 16.11.2018.

Sadržaj

1. OPIS REŠAVANOG PROBLEMA.....	3
2. TEORIJSKE OSNOVE.....	4
3. DIZAJN IMPLEMENTIRANOG SISTEMA.....	5
4. TESTIRANJE SISTEMA	6

1. OPIS REŠAVANOG PROBLEMA

Realizovati servis PubSubEngine koji služi za komunikaciju sa dve vrste klijenata: Publisher i Subscriber. Pri registraciji Publisher bira temu za koju će objavljivati alarmerne na koje se Subscriber-i pretplacuju. Alarmi se objavljuju na definisani vremenski period zajedno sa digitalnim potpisom.

Subscriber prilikom pretplate na neku temu bira opseg rizika za alarme izabrane teme. Subscriber prihvata alarme na koje je pretplacen i upisuje u internu bazu podataka. Proces prihvatanja alarma se loguje u Windows Event Log-u.

Autentifikacija se realizuje uz pomoc sertifikata. Tip validacije sertifikacije je custom. Custom validacija podrazumeva: Self-sign PubSubEngine sertifikat na osnovu kojeg se izdaju sertifikati za Publisher-a i Subscriber-a. PubSubEngine prilikom validacije proverava da li je klijentski sertifikat istekao I da li je on izdavalac tog sertifikata. Klijentska validacija podrazumeva proveru da li je sertifikat istekao , da li je self-signed I da li je CN odgovarajuci.

2. TEORIJSKE OSNOVE

Za izradu projekta koriscen je bezbednosni mehanizam **WCF komunikacija preko sertifikata**.

WCF komunikacija preko sertifikata

Kako bi se obezbedila adekvatna autentifikacija izmedju ucesnika u komunikaciji PubSubEngine-a, Publisher-a i Subscriber-a korisceni su sertifikati : PubSubEngine, Publisher, Subscriber i SignP.

- PubSubEngine – sastoji se od privatnog i javnog dela sertifikata (PubSubEngine.cer i PubSubEnding.pvk) I pretstavlja self-signed sertifikat. PubSubEngine.pfx se instalira u Personal folderu na racunaru na kojem se pokrece server. PubSubEngine.cer se instalira u Trusted Root Certification Authorities i u Trusted People na svim racunarima gde je potrebno obezbediti komunikaciju preko sertifikata. Ostali sertifikati se izdaju na osnovu njega. Klijenteske komponente prilikom validacija proveravaju da li je PubSubEngine self-signed, da li je istekao i da li je CN odgovarajuci.
- Publisher/Subscriber – sastoji se od privatnog I javnog dela sertifikata (Publisher/Subscriber.cer i Publisher/Subscriber.pvk). Publisher/Subscriber.pfx se instalira na racunaru na kojem se pokrece Publisher/Subscriber u folderu Personal. Server prilikom validacije proverava da li je sertifikat istekao i da li ga je PubSubEngine izdao.
- SignP – sastoji se od privatnog i javnog dela sertifikata (SignP.cer i SignP.pvk). SignP.pfx instalira se u Personal folderu na racunaru koji se pokrece kao Publisher, dok se SignP.cer instalira u Trusted People folderu na racunaru koji se pokrece kao Subscriber.

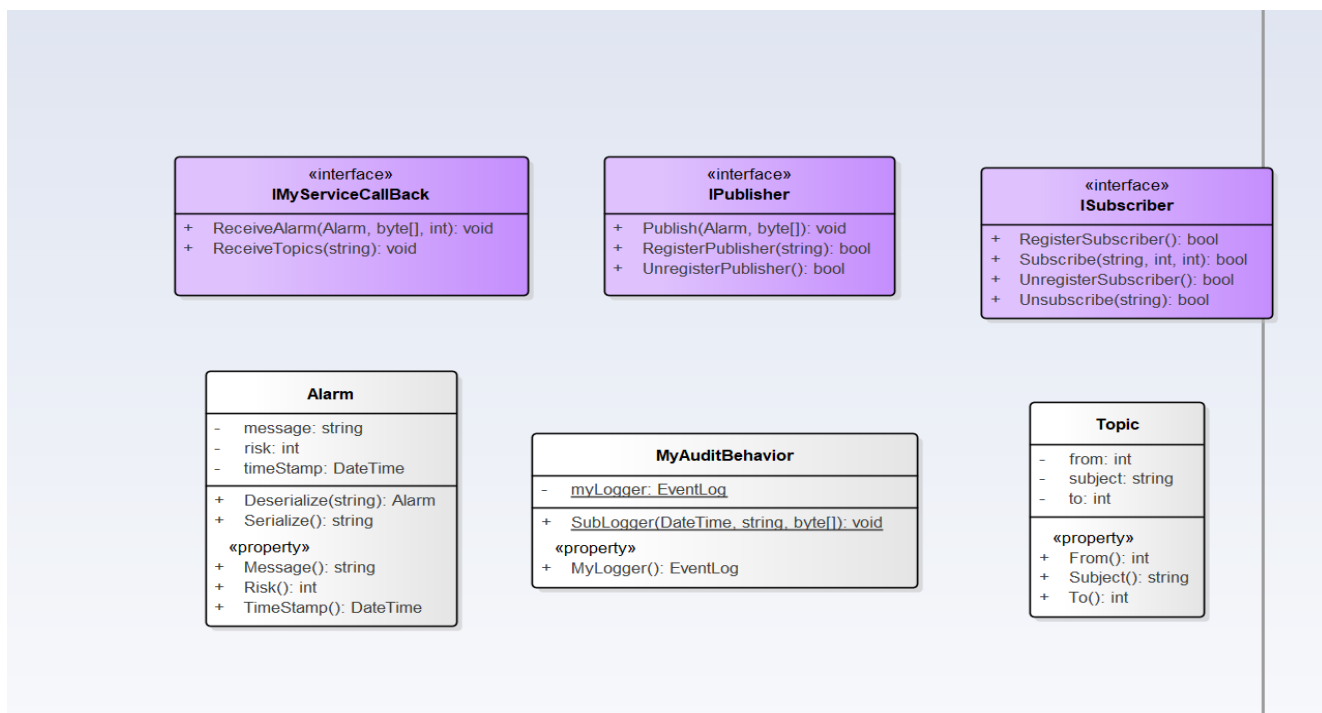
Digitalni potpis

Pomocu SignP sertifikata kreira se digitalni potpis za svaki od alarma. Alarm koji se salje se prvo serializuje, zatim se dobijena vrednost hash-uje SHA1 algoritmom, zatim se potpisuje privatnim kljucem SignP sertifikata.

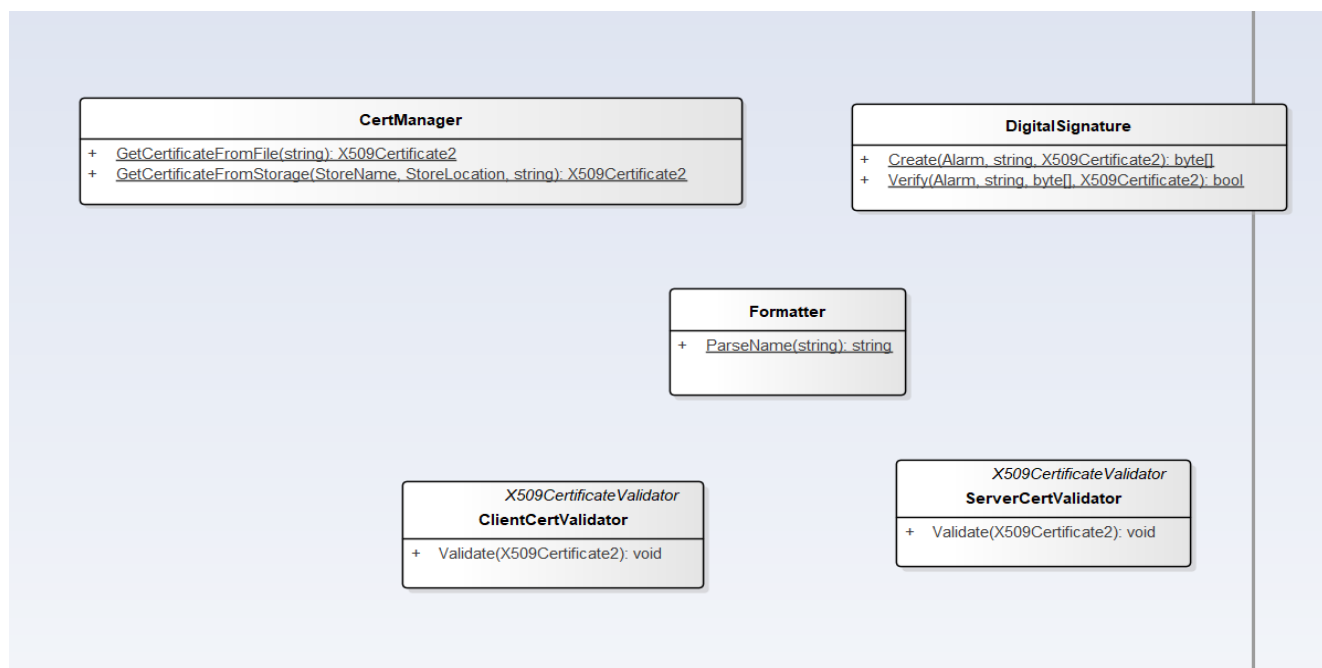
Sa druge strane, prilikom primanja alarma na strani Subscriber-a dobijeni alarm se ponovo serializuje, dobijena vrednost se hash-uje SHA1 algoritmom, zatim se uporedjuje sa dobijenim potpisom. U koliko su dobijene vrednosti jednake, verifikacija je uspesna.

3. DIZAJN IMPLEMENTIRANOG SISTEMA

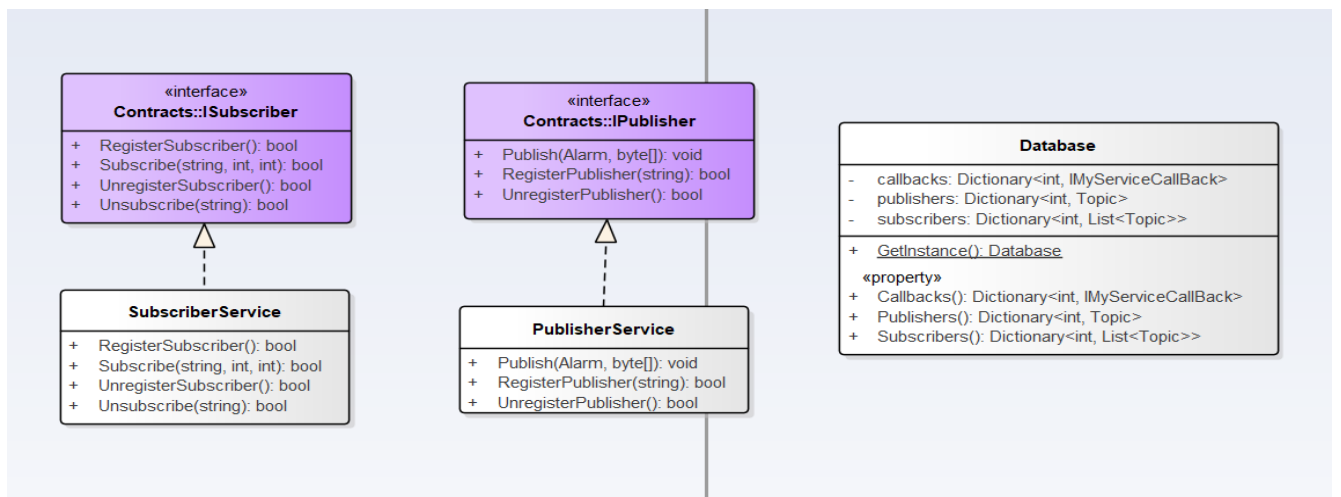
Arhitektura koriscenja u sistemu je WCF, tcp protokol. Bezbednosni mehanizam obezbedjen je koriscenjem sertifikata. Aplikacija “Contracts” izlaze interfejs klijentskim aplikacijama “Publisher” i “Subscriber”. Njih implementira serverska aplikacija “PubSubEngine”. Takodje, “Contracts” izlaze i interfejs za callback gde server poziva metode implementirane na klijentu “Subscriber”.



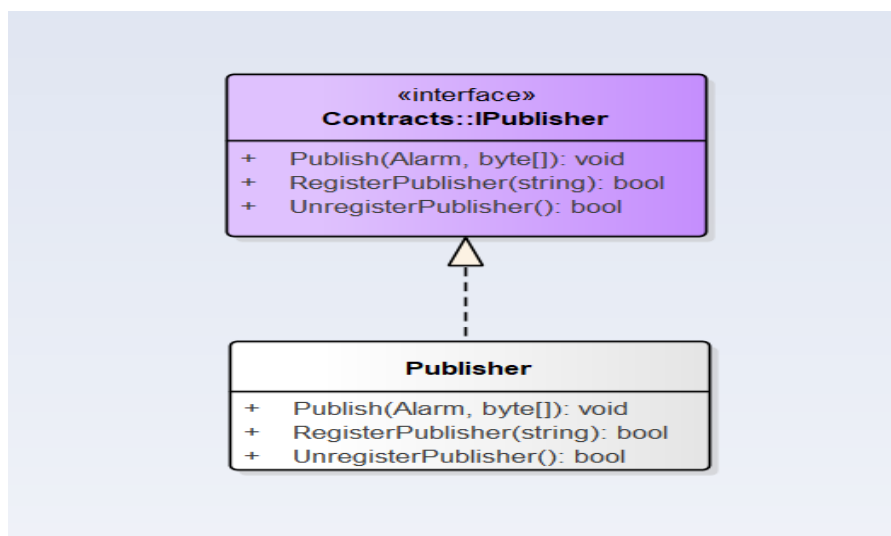
UML dijagram projekta “Contracts”



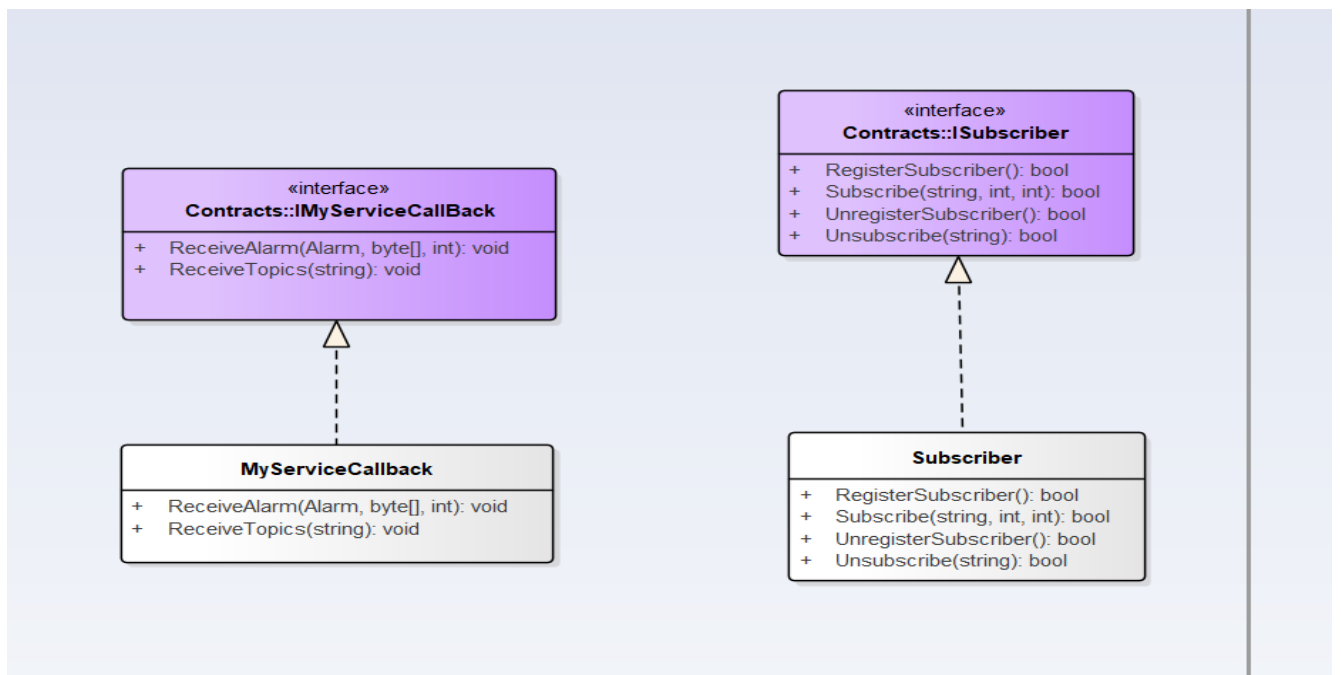
UML dijagram projekta “Manager”



UML diagram projekta “PubSubEngine”



UML diagram projekta “Publisher”

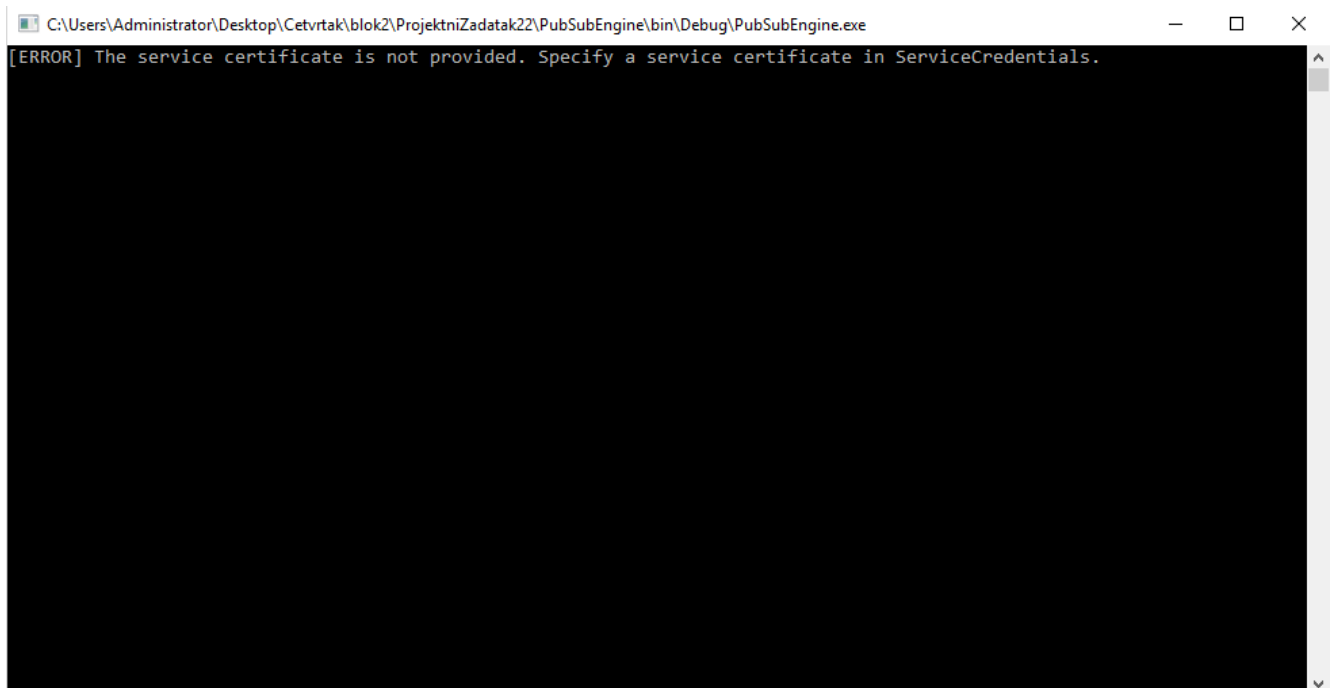


UML diagram projekta “Subscriber”

4. TESTIRANJE SISTEMA

Testirani su sledeci slucajevi:

- Pokretanje PubSubEngine-a kao Publisher/Subscriber
- Pokretanje PubSubEngine-a kao PubSubEngine
- Pokretanje Publisher-a/Subscriber-a kao Subscriber/Publisher respektivno
- Pokretanje Publisher-a/Subscriber-a kao Publisher/Subscriber respektivno



A screenshot of a Windows command prompt window. The title bar shows the file path: C:\Users\Administrator\Desktop\Cetvrtak\blok2\ProjektniZadatak22\PubSubEngine\bin\Debug\PubSubEngine.exe. The command prompt displays the following error message: [ERROR] The service certificate is not provided. Specify a service certificate in ServiceCredentials.

Pokretanje PubSubEngine-a kao Publisher/Subscriber



A screenshot of a Windows command prompt window. The title bar shows the file path: C:\Users\Administrator\Desktop\Cetvrtak\blok2\ProjektniZadatak22\PubSubEngine\bin\Debug\PubSubEngine.exe. The command prompt displays the following message: PubSubEngine is open. Press <enter> to finish...

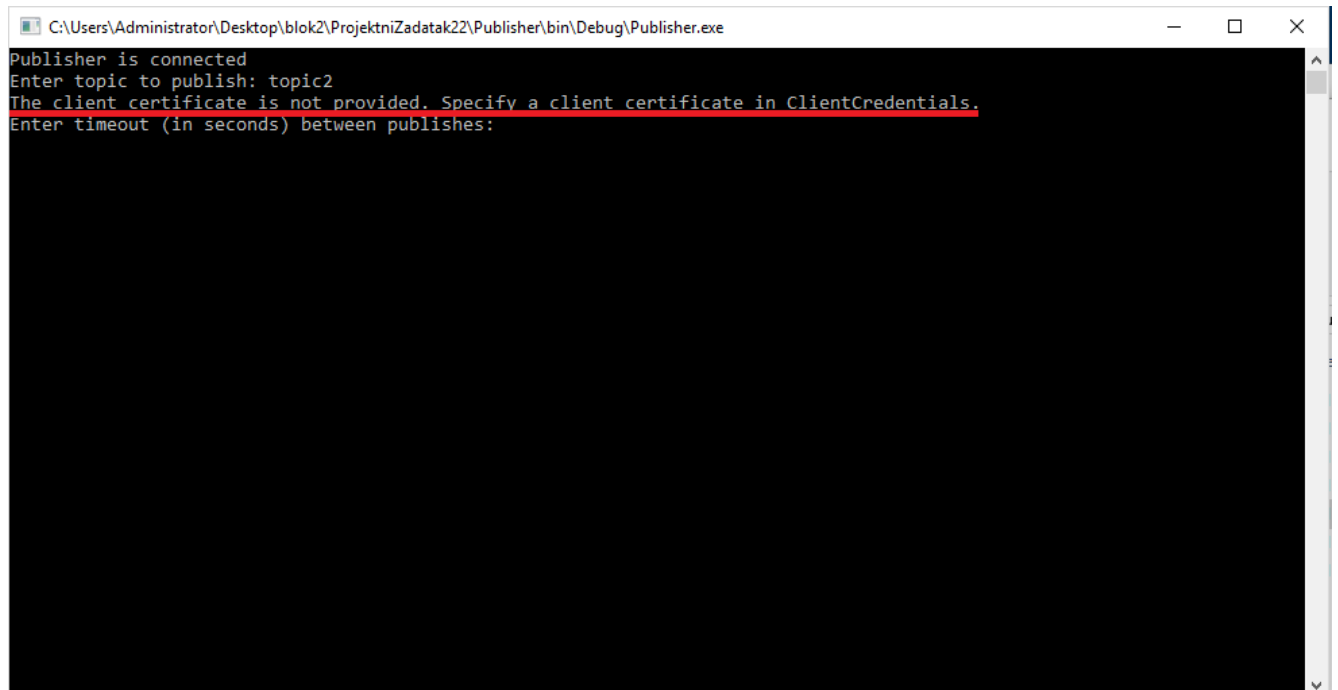
Pokretanje PubSubEngine-a kao PubSubEngine

```
C:\Users\Administrator\Downloads\blok2\blok2\ProjektniZadatak22\Subscriber\bin\Debug\Subscriber.exe
Connected to the PubSubEngine
*****Menu*****
1. Register
2. Unregister(and exit)
3. Subscribe
4. Unsubscribe
Choose option: 1
The client certificate is not provided. Specify a client certificate in ClientCredentials.
Failed to register.
*****Menu*****
1. Register
2. Unregister(and exit)
3. Subscribe
4. Unsubscribe
Choose option:
```

Pokretanje Publisher-a/Subscriber-a kao Subscriber/Publisher respektivno

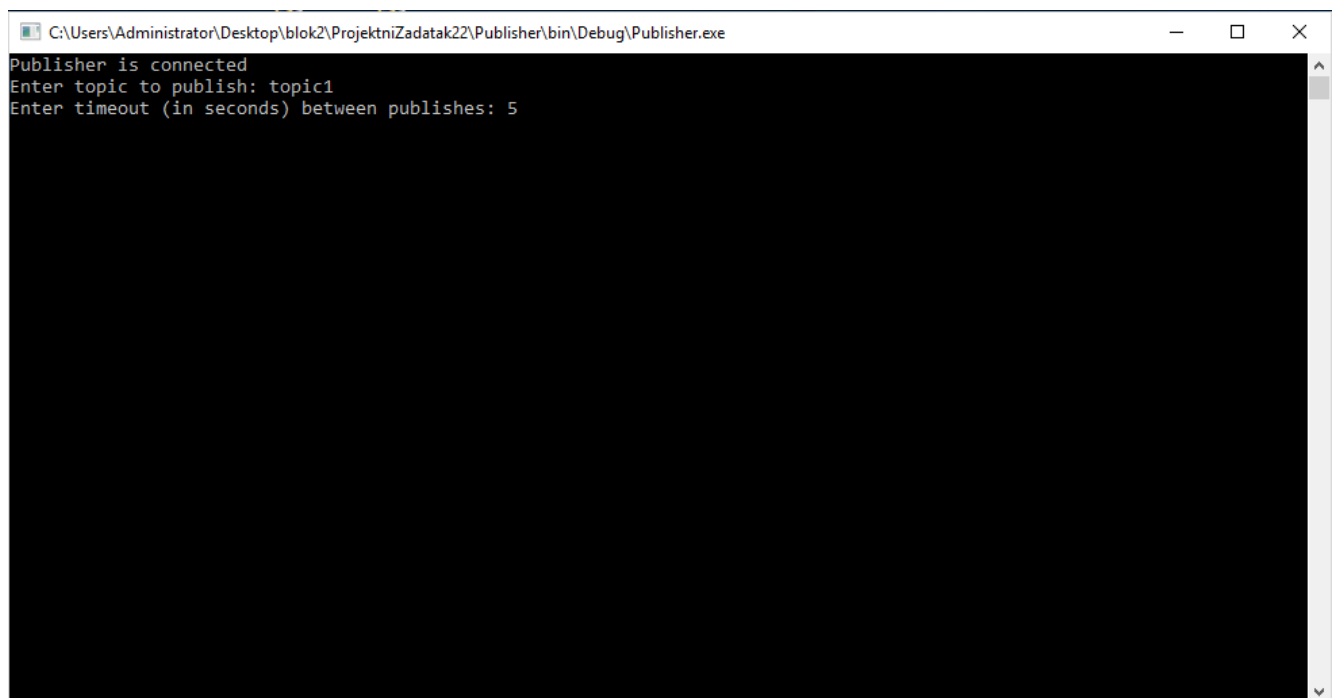
```
C:\Users\Administrator\Downloads\blok2\blok2\ProjektniZadatak22\Subscriber\bin\Debug\Subscriber.exe
Connected to the PubSubEngine
*****Menu*****
1. Register
2. Unregister(and exit)
3. Subscribe
4. Unsubscribe
Choose option: 1
Topics:
Successfully registered.
*****Menu*****
1. Register
2. Unregister(and exit)
3. Subscribe
4. Unsubscribe
Choose option:
```

Pokretanje Publisher-a/Subscriber-a kao Publisher/Subscriber respektivn



```
C:\Users\Administrator\Desktop\blok2\ProjektniZadatak22\Publisher\bin\Debug\Publisher.exe
Publisher is connected
Enter topic to publish: topic2
The client certificate is not provided. Specify a client certificate in ClientCredentials.
Enter timeout (in seconds) between publishes:
```

Pokretanje Publisher-a/Subscriber-a kao Subscriber/Publisher respektivn



```
C:\Users\Administrator\Desktop\blok2\ProjektniZadatak22\Publisher\bin\Debug\Publisher.exe
Publisher is connected
Enter topic to publish: topic1
Enter timeout (in seconds) between publishes: 5
```

Pokretanje Publisher-a/Subscriber-a kao Publisher/Subscriber respektivno