|  |  |  |
| --- | --- | --- |
|  | 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.

Sadrzaj

[1. OPIS REŠAVANOG PROBLEMA](#__RefHeading___Toc209_3190288126) 3

[2. TEORIJSKE OSNOVE](#__RefHeading___Toc211_3190288126) 4

[3. DIZAJN IMPLEMENTIRANOG SISTEMA](#__RefHeading___Toc321_3190288126) 5

[4. TESTIRANJE SISTEMA](#__RefHeading___Toc215_3190288126) 6

# OPIS REŠAVANOG PROBLEMA

Realizovati servis PubSubEngine koji sluzi za komunikaciju sa dve vrste klijenata: Publisher i Subscriber.Pri registraciji Pablisher bira temu za koju ce objavljivati alerme 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 serttifikacije 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.

# 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.

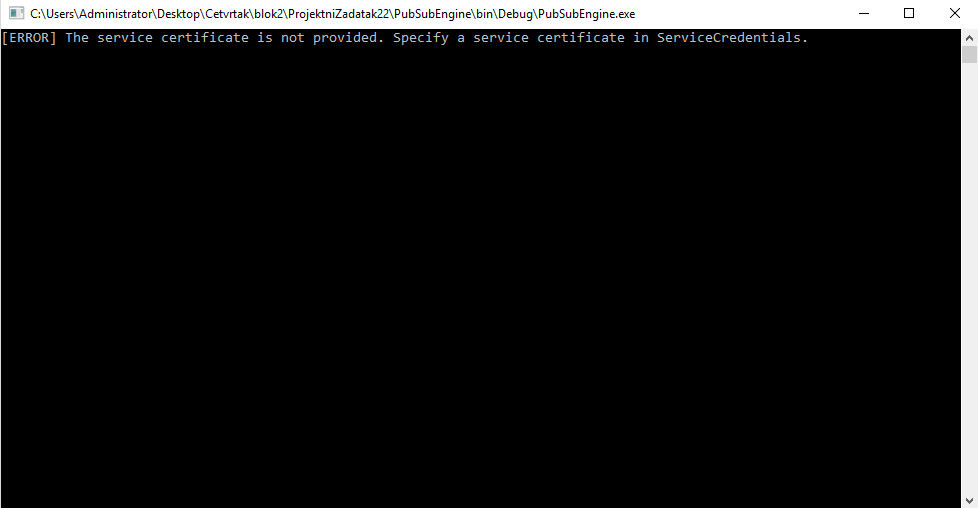
# DIZAJN IMPLEMENTIRANOG SISTEMA

Arhitektura i dizajn implementiranog sistema, kao i detaljan opis korišćenih komunikacionh protokola, interfejsa i bezbednosnih mehanizama. Prilikom kreiranja arhitekturalnog dijagrama neophodno je naglasiti koja komponenta izlaže koji interfejs, kao i koji je tip autentifikacije korišćen između komponenti.

# TESTIRANJE SISTEMA

Testirani su sledeci slucajevi:

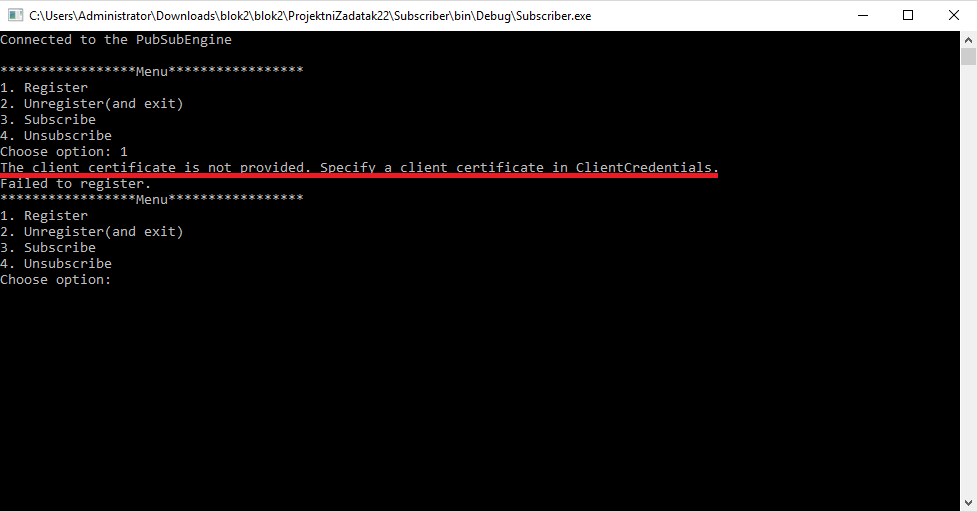
* Pokretanje PubSubEngine-a kao Publisher/Subscriber
* Pokretanje PubSubEngine-a kao PubSubEngine
* Pokretanje Publisher-a/Subscriber-a kao Subscriber/Publisher respektivno
* Pokretanje Publisher-a/Subscriber-a kao Publisher/Subscriber respektivno



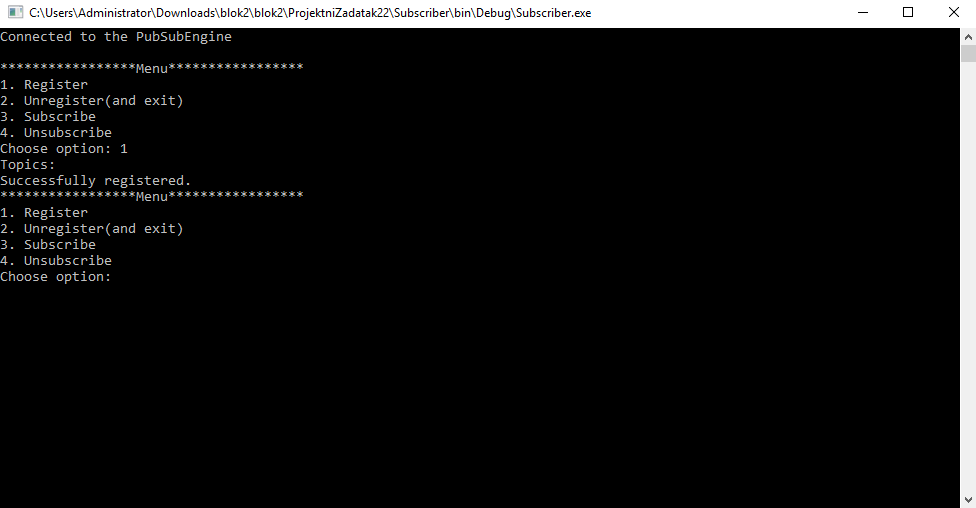
Pokretanje PubSubEngine-a kao Publisher/Subscriber



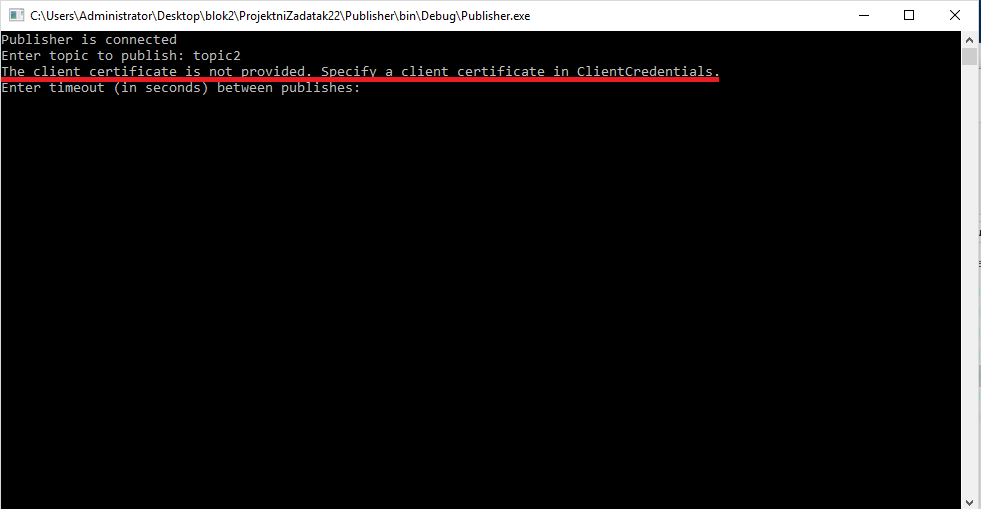
Pokretanje PubSubEngine-a kao PubSubEngine



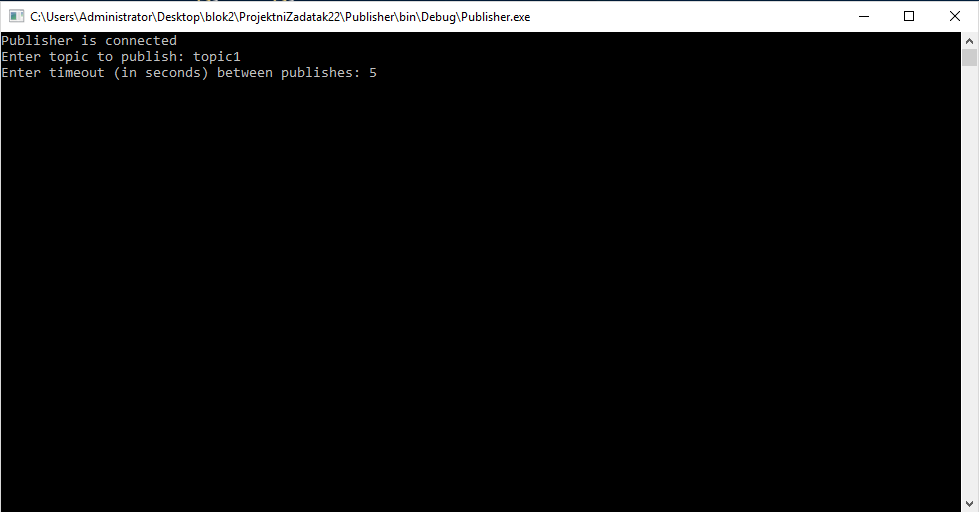
Pokretanje Publisher-a/Subscriber-a kao Subscriber/Publisher respektivno



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



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



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