|  |  |  |
| --- | --- | --- |
|  | UNIVERZITET U NOVOM SADU  FAKULTET TEHNIČKIH NAUKA  NOVI SAD |  |

Grupa 23

Đorđe Tošić PR26/2015,

Aleksandar Jančikin PR87/2015,

Bogdan Kovačev PR93/2015,

Petar Varga PR108/2015

Zadatak 3

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

Tema projektnog zadatka je komunikacija Client-a i Server-a, uz prethodnu validaciju njihovih sertifikata koje izdaje treća strana od poverenja tj. Certificate Manager Service.

Zadatak se sastoji iz 3 projekta:

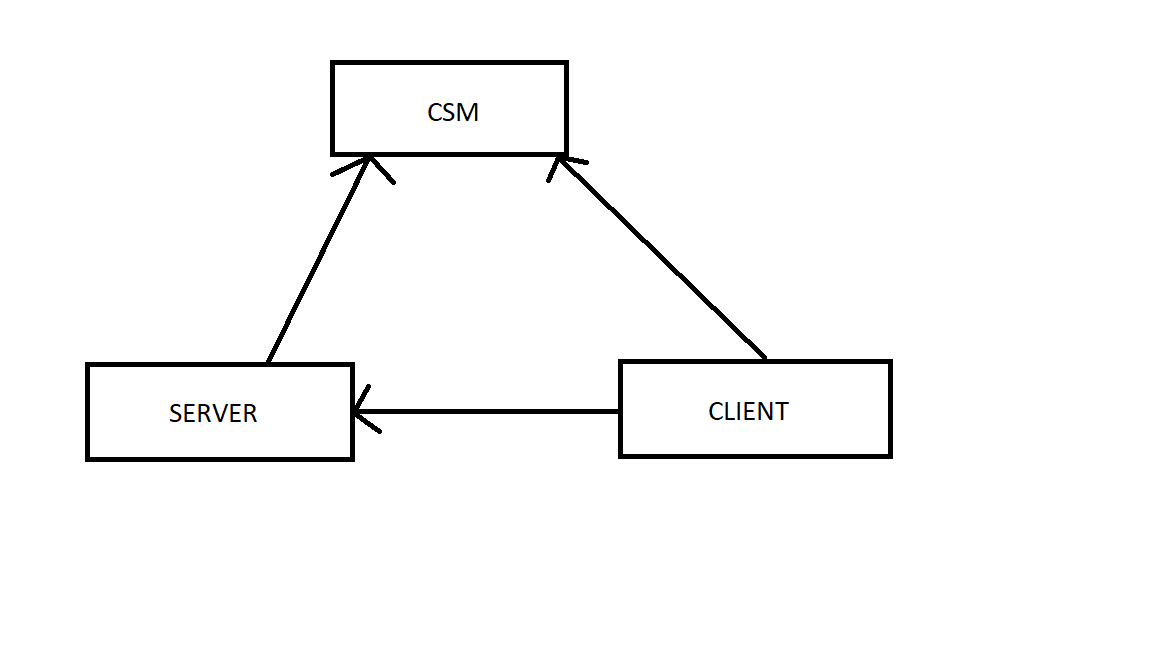
1. Server
2. Client
3. CMS
4. Common
5. Server je konzolna aplikacija koja funkcioniše tako što čeka da mu se Client obradi(nakon uspešne validacije njihovih sertifikata koje potpisuje CMS).
6. Client je konyolna aplikacija koja inicira komunikaciju sa Server-om(nakon uspešne validacije njihovih sertifikata koje potpisuje CMS).
7. CMS je konzolna aplikacija čije je zaduženje da izdaje sertifikate Client-ima i Server-u
8. Common predstavlja Class Library projekat, u kom su smesteni interface-i ostale stvari koje koriste sve tri strane.

Na početku pokretanja aplikacije Server i Client se obraćaju CSM-u radi potpisivanja njihovih sertifikata. U koliko su sertifikati validni Client započinje komunikaciju sa Server-om. Client se kači na Server na svaki proizvoljan broj sekundi ne veći od 10. Definisano u projektu zadatka neke akcije se upisuju u tekstualni fajl, a neke u Windows-ov Even Viewer.

# TEORIJSKE OSNOVE

Autentifikacija je proces u kome se dokazuju identiteti krajnjih učesnika u komunikaciji. Bezbednosni mehanizam korišćen u izradi projekta je korišćenje Sertifikata (komunikacija između klijenta i servera). Komunikacija klijent-server zasnovana je na sertifikatima. CMS izdaje sertifikate za servera i klijente. U sertifikat se ugradjuje javni ključ korisnika, dok se tajni ne razmenjuje. CMS komponenta svojim klijentima omogućuje generisanje sertifikata sa i bez privatnog ključa, omogućava povlačenje sertifikata u slučaju kompromitovanja I izdavanje novog sertifikata nakon kompromitovanja, omogućava validaciju izmedju klijentske i serverske strane gde se proverava Issuer (strana od poverenja koja je izdala sertifikate, tj CMS), proverava da li se sertifikati nalaze u listi povučenih sertifikata (RevocationList) i proverava da li je sertifikat istekao. CMS komponenta vrši i logovanje u okviru Windows event log-a. Ugrađeni .NET mehanizam za logovanje i audit koristi log datoteke Windows operativnog sistema za zapis različitih tipova događaja: sistemskih (generisanih od strane operativnog sistema), aplikativnih i bezbednosnih – tzv. Microsoft Windows Event Log. Dodatno .NET pruža mogućnost jednostavnog kreiranja novih log datoteka. Windows Event Viewer je alat za prikaz i upravljanje event logovima Windows operativnog sistema.

# DIZAJN IMPLEMENTIRANOG SISTEMA



Za komunikaciju između CMS-a sa serverom i klijentom koristi se interfejs ICMSCommunication sa metodama: Validate (validacija sertifikata), CreateAndSignCertificate (kreiranje i potpisivanje sertifikata), Withdrawal (povlačenje serifikata), GetCertificateFromStorage (dobavljanje sertifikata), CertificateExist (provera da li sertifikat postoji), NumOfCertificates (broji valide i nevalidne sertifikate određenog klijenta). Za komunikaciju između klijenta i servera koristi se interfejs IWCFContract sa metodom: TestCommunication.

# TESTIRANJE SISTEMA