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

Grupa 27

Saša Dragomirović PR75/2015 Mladen Milošević PR 77/2015

Milan Falčić PR 122/2015

Zadatak 26

Sigurnost i bezbednost u elektroenergetskim sistemima

* Primenjeno softversko inženjerstvo -

Novi Sad, 13.11.2018

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

Implementirati BankingService komponentu koja podržava dva interfejsa:

IUserServices i IAdminServices.

IuserService je namenjen ya rad sa klijentima koji žele da otvore račun u banci,da podignu kredit, ili da izvrše transakciju (uplatu/isplatu) na svom računu.

IadminService je interfejs namenjen za administratore koji kreiraju bazu podataka za skladištenje svih pristiglih zahteva i periodičnoproveravaju zastarelost pristiglih zahteva.Zahtev se smatra zastarelim ukoliko je u bazi duže od unapred definisanog perioda, i u tom slučaju administrator ga uklanja.

Banka ima tri sektora:

1. IT sektor za otvaranje računa
2. Sektor za podizanje kredita
3. Sektor za transakcije ( uplate i isplate)

Nakon što novi zahtev pristigne, BankingService prosleđuje zahteve sektorima na obradu.Zahtevi se po dospeću upisuju u bazu podataka gde se vodi evidencija o svim zahtevima, i prosleđuje se na obradu kada se odgovarajući sektor oslobodi.Klijent se obaveštava o izvršenoj obradi zahteva,bilo uspešnoj obradi ili odbijenom zahtevu.

Autentifikacija između banke i njenih sektora je preko Windows Authentification protokola, a njihova komunikacija treba da obezbedi samo integritet podataka (ne i poverljivost).

Za autentifikaciju između svih klijenata i BankingService komponente koriste se sertifikati, a validacija se vrši po pravilu lanca poverenja. Dodatno, metode interfejsa IUserServices i IAdminServices je potrebno zaštiti u skladu sa korisničkom ulogom koja je definisana atributom OU (Organizational Unit) u okviru SubjectName vrednosti sertifikata svakog korisnika.

Sve akcije u sistemu počev od autentifikacije, autorizacije, kao i rad nad samom bazom podataka potrebno je logovati u okviru specifičnog log fajla u okviru Windows Event log-a.

# TEORIJSKE OSNOVE

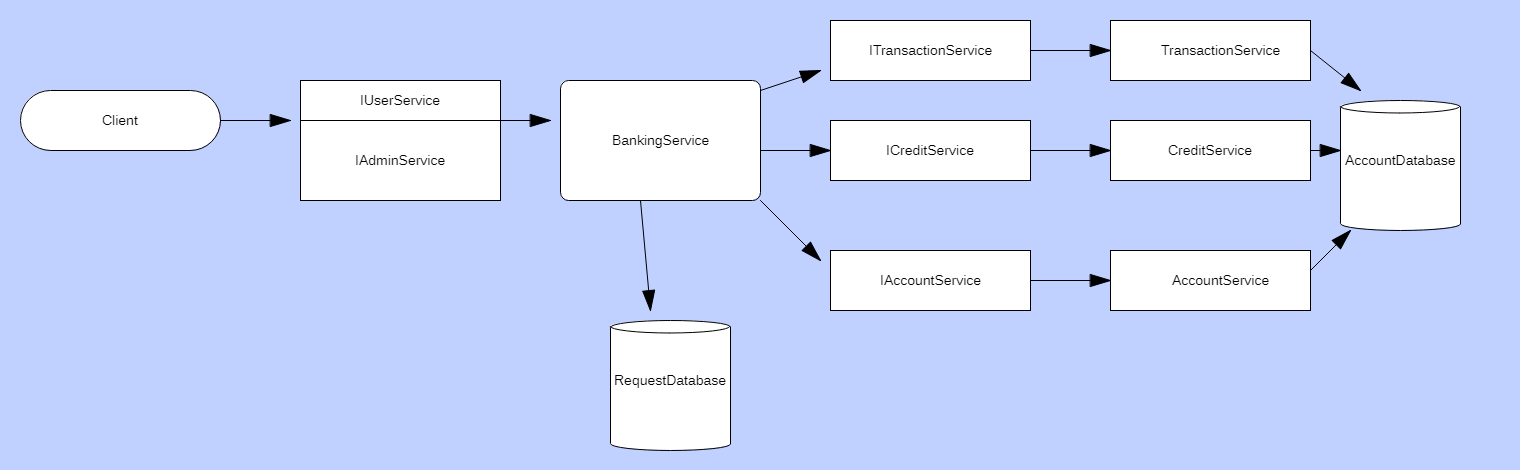
Za *BankingService* je korišćeno više bezbednosnih mehanizama.

Za autentifikaciju između servisa banke i njenih sektora je korišten ugrađeni Windows autentifikacioni protokol i njihovom komunikacijom je obezbeđen integritet podataka. *Binding* je WCF mehanizam kojim se definiše način komunikacije između klijenta i servisa. WCF nudi širok spektar ugrađenih bindinga, dok je u zavisnosti od specifičnih zahteva aplikacije njihova podešavanja moguće izmeniti ili definisati specifične (custom) bindinge. WCF bindingom se specifiira komunikacioni protokol, bezbednosni mod (Transport Security i Message Security) i format poruke koja se razmenjuje.

Za autentifikaciju između svih klijenata i *BankingService* komponente koriste se sertifikati, a validacija se vrši po pravilu lanca poverenja. Dodatno, metode interfejsa *IUserServices* i *IAdminServices* su zaštićene u skladu sa korisničkom ulogom koja je definisana atributom OU *(OrganizationalUnit)* u okviru *SubjectName* vrednosti sertifikata svakog korisnika. Sertifikat predstavlja digitalni identitet korisnika izdat od strane sertifikacionih tela (*certification authority, CA*).

Sertifikat sadrži različite podatke: podaci o vlasniku sertifikata (*Subject*), validnost odnosno period važenja sertifikata (*ValidFrom, ValidTo*), informacije o izdavaocu sertifikata (*Issuer*). U sertifikat se ugrađuje javni ključ korisnika (uz identifikator algoritma primenjenog za generisanje ključa, npr. *RSA*), dok se tajni ključ ne razmenjuje. Svaki sertifikat je digitalno potpisan od strane sertifikacionog tela koje ga izdaje čime se potvrđuje da sertifikat zaista pripada podnosiocu zahteva.

# DIZAJN IMPLEMENTIRANOG SISTEMA



Klijent se radi usluge obraća BankingService-u preko interfejsa IUserService ili IAdmintService, u zavisnosti da li se klijent autentifikuje kao User ili Admin. Autentifikacija i autorizacija između klijenta i servisa vrši preko sertifikata. BankingService implementira interfejse IUserService i IAdminService.Klijentovi zahtevi se upisuju u bazu podataka (baza je JSON file) koja čuva sve zahteve korisnika. Upisani zahtevi sadrže polje koje označava da li je zahtev obrađen ili se nalazi u redu čekanja. Zahtev se nalazi u redu čekanja ako je traženi sektor zauzet. BankingService pristupa sektorima preko interfejsa IAccountService, ITransactionService i ICreditService u zavisnosti koji je sektor potreban klijentu.

AccountService implementira IAccountService interfejs i pruža mogućnost otvaranja novog ručuna u banci. Račun se nakon otvaranja upisuje i čuva u bazu podataka AccountDatabase.Svaki account (račun) sadrži ime klijenta, jedinstveni identifikator (ID), stanje na računu i kreditno dugovanje.

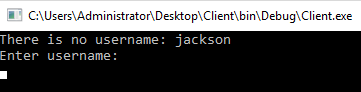
CreditService implementira ICreditService interfejs i omogućava korinicima dizanje kredita.

TransactionService implementira ITransactionService i omogućava korisnicima uplatu novca na račun, kao i podizanje novca sa računa. Prilikom uplate na račun, ukoliko klijent poseduje kredit, tj. klijent se zadužio u banci, 50 % svake uplate oduzima se radi otplate kredita.

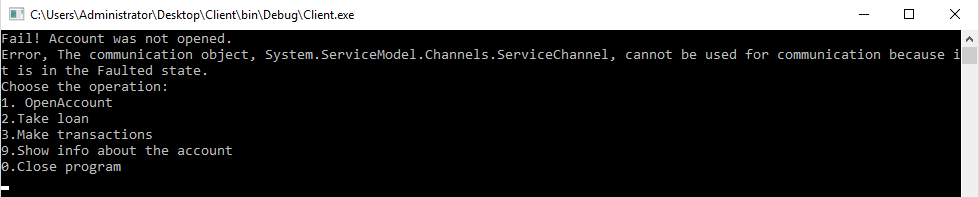
Klijent logovan kao Admin kreira bazu podataka za zahteve, ukoliko ne postoji, i periodično proverava da li je zahtev zastareo.Zastareli zahtevi se brišu iz baze podataka i klijentu se daje do znanja da je njegov zahtev izbrisan i nije odrađen.

Autentifikacija između banke i njenih sektora vrši preko Windows Authentification protokola, dok se autentifikacija i autorizacija između klijenta i banke tj. njenih sektora, vrši uz pomoć sertifikata.

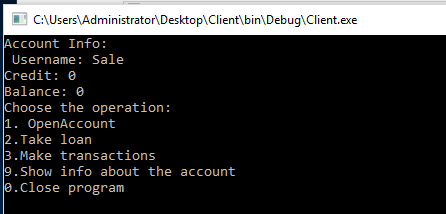
# TESTIRANJE SISTEMA



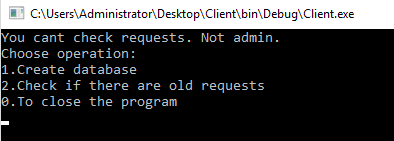
1- Ukoliko korisnik nema sertifikat, ne moze se konektivati na servis



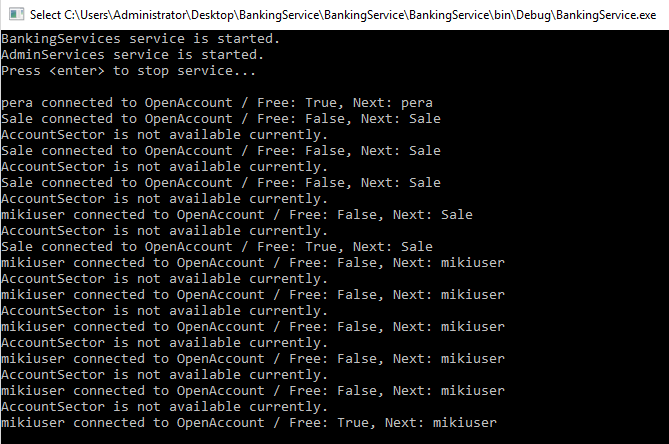
2- Ukoliko korisnikov sertifikat nema isti CA kao servis, ne moze se konektovati



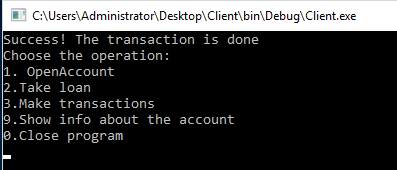
- Ukoliko je korisnik autentifikovan i autorizovan, moze zatraziti informacije o svom racunu



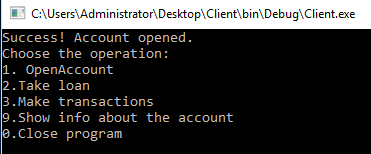
- Ukoliko se korisnik pokusa prijaviti kao Admin, a nije autorizovan za admin akcije, onda mu prikaze poruku da nema prava



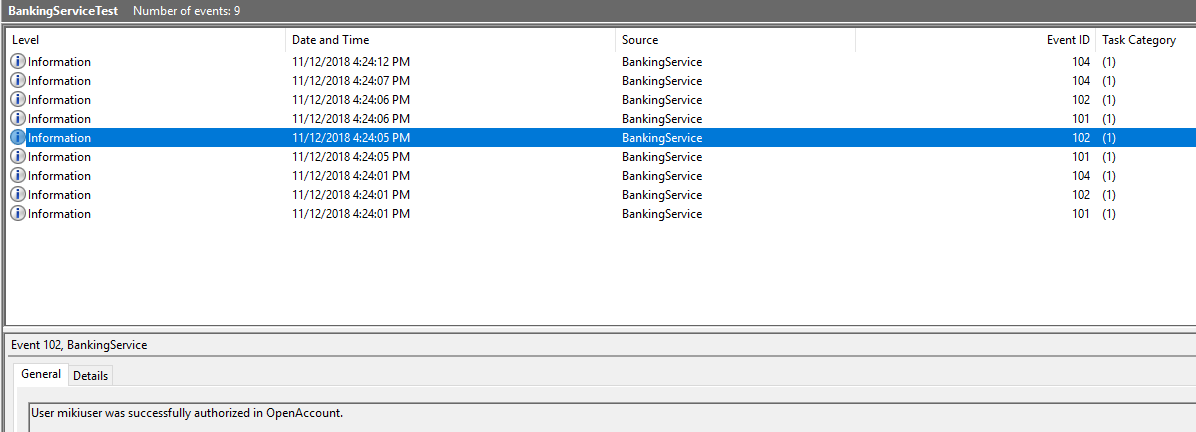
- Primer kad se prikljuce tri razlicita korisnika i cekaju u redu za otvaranje racuna jer sektor nije slobodan



- Ukoliko je korisnik autentifikovan i autorizovan moze da izvrsi odredjene akcije nad svojim racunom



- Primer uspesnog otvaranja racuna korisnika



- EventViewer za sve korisnikove akcije i rad nad bazom podataka