Projektni zadatak 28.

Implementirati servis za upravljanje bazom podataka koja sadrži poverljive podatke kriptovane tajnim ključem servisa, a koji se generiše prilikom startovanja servisa, primenom AES simetričnog algoritma. Baza podataka (txt fajl) sadrži događaje generisane od strane validnih korisnika. Spisak validnih događaja je unapred definisan (u okviru resursnog fajla), dok se u bazu podataka uz odgovarajuću poruku skladište informacije:

- jedinstveni identifikator entiteta u bazi podataka,
- jedinstveni identifikator klijenta koji generiše događaj,
- Timestamp kad je dati događaj izgenerisan.

Klijenti i servis se obostrano autentifikuju posredstvom sertifikata (*ChainTrust*), nakon čega servis razmenjuje tajni kluč sa klijentom tako da samo taj klijent može da ga dekriptuje. Koristeći ovaj tajni ključ svaki klijent može interno da pristupi bazi podataka i dekriptuje je.

Dodatno, servis omogućuje klijentima sledeće akcije nad bazom podataka:

- ažuriranje sadržaja baze podataka - ukoliko korisnik ima Update permisiju,
- dodavanje novog entiteta u bazu - ukoliko korisnik ima Add permisiju,
- uklanjanje postojećeg entiteta iz baze - ukoliko korisnik ima Delete permisiju.

Implementirati RBAC model koji se zasniva na korisničkim ulogama u sistemu definisanim uz pomoć *SubjectName* atributa *OrganizationalUnit*.

Sve pokušaje uspešnog i neuspešnog pristupa bazi servis loguje u custom kreiranom Windows Event Logu. Ukoliko se nad istim entitetom detektuje N (konfigurabilno) neuspešnih pokušaja izmene ili brisanja u periodu od M (konfigurabilno) minuta/sekundi, servis šalje alarm Intrusion Detection System (IDS) servisu koji generiše (ispisuje na konzoli) alarm. Komunikacija između servisa i IDS komponenete se ostvaruje putem Windows autentifikacionog protokola.