Projektni zadatak 6.

Implementirati bankarski sistem koji se sastoji od sledećih komponenti:

- BANKA ima dve uloge:
    - Izdavanje MasterCard kartica svojim klijentima prilikom kreiranja računa. Za potrebe izdavanja kartice klijenti kontaktiraju banku putem Windows komunikacionog protokola. MasterCard je sertifikat generisan tako da *SubjectName* odgovara korisničkom imenu, a dodatno se definiše i PIN kod kao drugi faktor autentifikacije (koji banka ne sme da skladišti u čitljivom formatu). Izgenerisane kartice se čuvaju u lokalnom folderu za potrebe kasnijeg distribuiranja. Distribucija MasterCard sertifikata se vrši ručno.
    - Upravljanje korisničkim transakcijama, odnosno uplate i isplate, kada se klijenti predstavljaju banci putem sertifikata. Svaka transakcija mora biti digitalno potpisana od strane klijenta.
- KLIJENTI, koji:
    - Šalju zahteve za kreiranje naloga, zahteve za povlačenje sertifikata i izdavanje novog u slučaju kompromitovanja. U ovom slučaju klijenti sa bankom uspostavljaju komunikaciju preko Windows autentifikacionog protokola.
    - Šalju zahteve za izvršenje transakcije i za reset PIN koda, kada se korisnici i banka međusobno autentifikuju korišćenjem sertifikata. Prilikom slanja svake transakcije, vrši se validacija PIN koda, kao i validacija digitalnog potpisa.
- Repliciranje podataka o svim korisničkim nalozima na backup server. Primarna i backup komponenta za upravljanje sertifikatima se autentifikuju koristeći Windows autentifikacioni protokol.

Dodatno, BANKA vodi evidenciju o svim aktivnostima KLIJENATA u okviru specifičnog kreiranog Windows event loga, pre svega sledeće aktivnosti:

- Zahtevi za izdavanje, povlačenje i obnavljanje MasterCard sertifikata,
- Izvršene uplate i isplate,
- Zahtevi za reset PIN koda MasterCard sertifikata,
- Zahtevi za izvršavanje transakcija.

Poruke koje se razmenjuju izmedju klijenata i banke treba da budu kriptovane 3DES algoritmom u EBC modu i digitalno potpisane. Dodatno, ukoliko BANKA detektuje da je u periodu od N (konfigurabilno) vremena detektovana transakcija isplate na istom računu više od M puta, prijavljuje događaj centralnom BankingAudit serveru sa kojim komunicira preko Windows autentifikacionog protokola. Prilikom logovanja neophodno je kao Source navesti ime banke, naziv računa, vreme detektovanja i iznose transakcija.