Projektni zadatak – SCS

Implementirati komponentu za upravljanje karticama (SmartCardsService) koja će čuvati podatke o karticama korisnika. Podaci koji se nalaze u smart kartici su korisničko ime korisnika koje treba upisati u polje SubjectName i šifra koja predstavlja 4-cifreni PIN kod. Izgenerisane kartice se čuvaju i u lokalnom folderu za potrebe kasnijeg distribuiranja. PIN kod se ne sme skladištiti u plaintextu već u formatu SHA-2 hash vrednosti.

Neophodno je da ovaj servis replicira podatke na backup server. Primarna i backup komponenta za upravljanje smart karticama se autentifikuju koristeći Windows autentifikacioni protokol.

Svi korisnici Smart kartica uspostavljaju komunikaciju sa SCS komponentom putem Windows autentifikacionog protokola, i mogu pripadati SmartCardUser ili Manager grupi. Ovi podaci se takođe integrišu u okviru sertifikata (polje OrganizationalUnit). Omogućiti klijentima da menjaju PIN kod.

Replikacija podataka u SmartCardsService kao i menjanje PIN koda treba da se loguju u okviru custom generisanog Windows event loga.

Razviti WCF klijent-servis model takav da ulogu servisa ima ATM komponenta koja realizuje uplate i isplate za korisnika. Korisnik se autentifikuje ATM komponenti preko 2-faktor autentifikacije: prvi faktor je smart kartica, a drugi faktor je PIN kod za šta se ATM obraća SmartCardsService komponenti za validaciju PIN koda. ATM se autentifiukje klijentu sertifikatom (ChainTrust) izdatim od strane SmartCardsService komponente takođe. Korisniku je dozvoljeno da izvrši ovu akciju ukoliko je sertifikovan da bude SmartCardUser. Distribucija i generisanje sertifikata se vrši ručno.

ATM nudi mogućnost ispisa svih aktivnih korisničkih naloga, ali je to dozvoljeno samo korisnicima koji su sertifikovani kao Manageri.

Sve poruke između klijenata i ATM komponente moraju biti digitalno potpisane.

Dodatno, ATM servis treba da vodi evidenciju o svim aktivnostima klijenata u okviru Application Windows event loga: 1) o izvršenim uplatama 2) o izvršenim isplatama.