Elektrotehnički fakultet Banja Luka
Katedra za računarsku tehniku i informatiku
Kriptografija i računarska zaštita
Projektni zadatak

Zadatak

Napisati aplikaciju koja predstavlja siguran repozitorijum za skladištenje povjerljivih dokumenata. Aplikacija treba da omogući skladištenje dokumenata za veći broj korisnika tako da je pristup određenom dokumentu dozvoljen samo njegovom vlasniku.

Korisnici se prijavljuju na sistem kroz dva koraka. U prvom koraku je potrebno unijeti digitalni sertifikat koji svaki korisnik dobija prilikom kreiranja naloga. Ukoliko je sertifikat validan, korisniku se prikazuje forma za unos korisničkog imena i lozinke. Nakon uspješne prijave, korisniku je kroz proizvoljno realizovan interfejs dostupan spisak njegovih dokumenata.

Aplikacija omogućava korisniku opciju preuzimanja postojećih dokumenata kao i *upload* novih dokumenata. Svaki novi dokument se, prije smiještanja na fajl-sistem, dijeli na N segmenata ($N \geq 4$, slučajno generisana vrijednost), pri čemu se svaki od tih segmenata smiješta u različit direktorijum, kako bi se dodatno povećala sigurnost sistema i smanjila mogućnost krađe dokumenata. Potrebno je na adekvatan način zaštititi tajnost i integritet svakog segmenta, tako da jedino korisnik kome pripada dokument može da dođe u njegov posjed i vidi njegov sadržaj. Aplikacija treba da detektuje svaku neovlaštenu izmjenu uskladištenih dokumenata i obavijesti korisnika o tome, prilikom pokušaja preuzimanja takvih dokumenata.

Aplikacija podrazumijeva postojanje infrastrukture javnog ključa. Svi sertifikati treba da budu izdati od strane CA tijela koje je uspostavljeno prije početka rada aplikacije. Podrazumijevati da će se na proizvoljnoj lokaciji na fajl-sistemu nalaziti CA sertifikat, CRL lista, sertifikati svih korisnika, kao i privatni ključ trenutno prijavljenog korisnika (nije potrebno realizovati mehanizme za razmjenu ključeva). Potrebno je ograničiti korisničke sertifikate tako da se mogu koristiti samo u svrhe koje zahtijeva aplikacija. Pored toga, podaci u sertifikatu treba da budu povezani sa odgovarajućim korisničkim podacima. Korisnički sertifikati se izdaju na period od 6 mjeseci. Osim toga, ukoliko korisnik u toku jedne prijave unese pogrešne kredencijale tri puta, njegov sertifikat se automatski suspenduje i aplikacija mu prikazuje odgovarajuću poruku. Nakon toga, aplikacija nudi korisniku opciju reaktivacije sertifikata (ukoliko unese ispravne kredencijale), ili registracije novog naloga.

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Dozvoljena je upotreba proizvoljnog programskog jezika i odgovarajuće biblioteke za realizaciju kriptografskih funkcija (npr. *Bouncy Castle*). Način realizacije korisničkog interfejsa neće biti ocjenjivan.

Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2023. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.