Druga domaća zadaća iz Posrednika umreženih sustava

Cilj zadatka je izgraditi složeni sustav sa N pružatelja usluga (SP – Service Provider) i 1 središnjim registrom (CR – Central Registry).

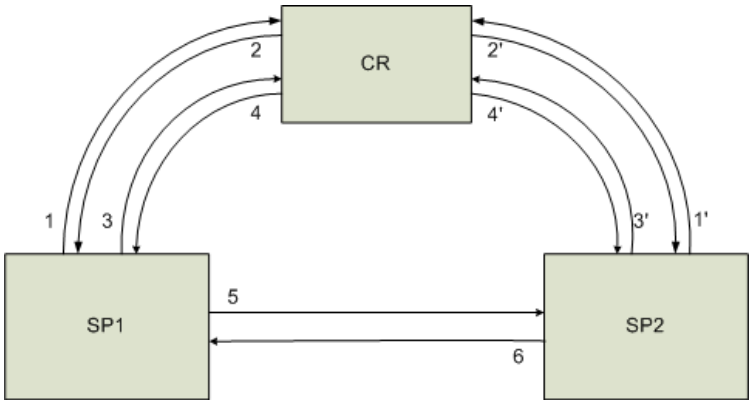
Pružatelji usluga pružaju uslugu rada nad datotekama podataka. Svaki pružatelj usluga ima svoje korisnike i datoteke svojih korisnika. Pored toga, pružatelji usluga pružaju svojim korisnicima i mogućnost rada sa datotekama drugih pružatelja usluga koji su prijavljeni u središnji registar.
Zadatak je razviti pružatelje usluga (barem dva) sa opisanom funkcionalnosti. Radi jednostavnosti zadatka, pretpostavite da je jedina moguća operacija nad datotekama operacija čitanja. Dakle, nema operacije pisanja i stvaranja datoteka, nego pretpostavite da su sve datoteke u sustavu već stvorene. Možete pretpostaviti i da se radi samo o tekstualnim datotekama. Također, možete pretpostaviti da su i svi korisnici u sustavu već registrirani (tj. ne treba ugraditi podršku za prijavu novih korisnika).

Središnji registar sadrži liste *Lista pružatelja usluga* i *Lista datoteka*. U *Listi pružatelja usluga* za svakog postojećeg pružatelja usluge pamti se ID, naziv i adresa pružatelja usluge. U *Listi datoteka* svih javno dostupnih datoteka svim korisnicima bilo kojeg pružatelja usluge pamti se ID datoteke, naziv datoteke, autor datoteke, kratki opis datoteke i ID pružatelja usluge koji poslužuje dotičnu datoteku.
Zadatak je razviti središnji registar sa opisanom funkcionalnosti. Razvijeni registar mora imati izložena programska sučelja (API) za dohvat *Liste pružatelja usluga* i *Liste datoteka*.

Osim navedenih, glavni zadatak je razviti ***posrednički sloj*** kojeg će koristiti pružatelji usluga kako bi ostvarili funkcionalnost rada sa datotekama. Posrednički sloj obuhvaća sljedeće:

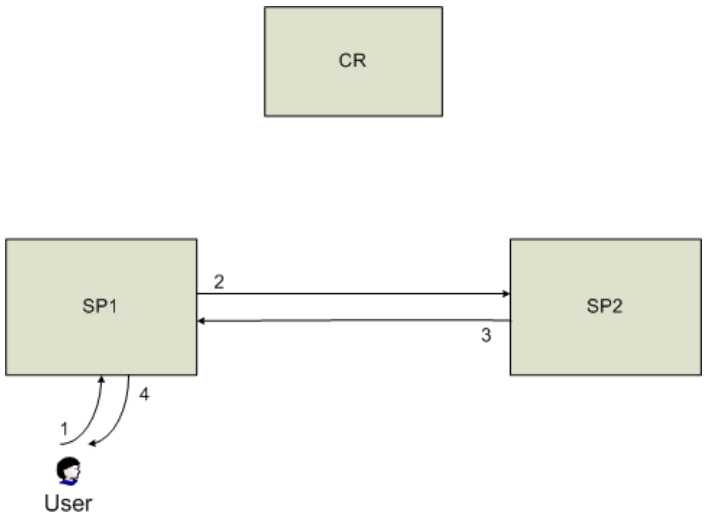
a) Podsustav za prijavu pružatelja usluge u središnji registar
   - na početku svoga rada, pružatelj usluge prijavljuje se u središnji registar kako bi bio vidljiv drugim prijavljenim pružateljima usluga
b) Podsustav za prijavu datoteka u središnji registar
   - pružatelj usluge s vremena na vrijeme (radi jednostavnosti zadatka, može biti samo na početku rada) prijavljuje datoteke koje pohranjuje u središnji registar kako bi bile vidljive drugim prijavljenim pružateljima usluga (odnosno njihovim korisnicima)
c) Podsustav za dohvat popisa datoteka iz središnjeg registra
   - pružatelja usluge s vremena na vrijeme (radi jednostavnosti zadatka, može biti samo na početku rada) dohvaća popis datoteka iz središnjeg registra kako bi ih na zahtjev korisnika mogao prikazati korisniku
d) Podsustav za lokalni dohvat datoteke
   - pružatelj usluge na zahtjev korisnika dohvaća lokalno iz svog spremišta datoteku ako se tražena datoteka nalazi na tom lokalnom pružatelju usluge
e) Podsustav za uspostavu infrastrukture javnog ključa

- u sustavu sadržanom od pružatelja usluga i središnjeg registra uspostavlja se infrastruktura javnog ključa kako bi se osigurao siguran dohvat udaljenih datoteka
- središnji registar je Certificate Authority koji izdaje certifikate pružateljima usluga



1. Pružatelj usluga SP1 šalje zahtjev središnjem registru CR za digitalnim certifikatom CR-a.
2. Središnji registar CR dohvaća svoj certifikat iz svog lokalnog spremnika i šalje ga pružatelju usluge SP1, koji ga sprema za buduću provjeru vjerodostojnosti certifikata ostalih SP-ova (na osnovu javnog ključa koji piše u certifikatu).
3. Pružatelj usluge SP1 šalje zahtjev središnjem registru CR za stvaranjem digitalnog certifikata SP1.
4. Središnji registar CR potpisuje svojim privatnim ključem dobiveni zahtjev stvarajući tako vjerodostojni certifikat SP1. Središnji registar sprema certifikat SP1 u svoj lokalni spremnik.
   *** prva 4 koraka obavljaju svi SP-ovi kada kreću s radom (pa su koraci označeni sa crticom) ***
5. Prije prve komunikacije između dva SP-a, mora se obaviti razmjena certifikata tih SP-ova kako bi bili uvjereni u istinitost identiteta drugog SP-a i imali pristup njegovom javnom ključu. Pružatelj usluge SP1 šalje zahtjev pružatelju usluge SP2 za certifikatom SP2 i šalje svoj certifikat SP1.
6. Pružatelj usluge SP2 dohvaća svoj certifikat iz svog lokalnog spremnika i šalje ga pružatelju usluge SP1. Po primitku certifikata SP2, pružatelj usluge SP1 provjerava njegovu vjerodostojnost koristeći javni ključ certifikata CR (dobivenog u koraku 2). Isto čini i pružatelj usluga SP2 sa certifikatom SP1 kojeg je dobio prilikom primopredaje u koraku 5.
   *** koraci 5-6 ne moraju se odviti odmah nakon koraka 4, već u bilo kojem vremenskom trenutku kasnije kada se uspostavlja prvi put komunikacija između neka dva SP-a ***

f) Podsustav za udaljeni dohvat datoteke
- pružatelj usluge na zahtjev korisnika dohvaća traženu datoteku iz spremišta udaljenog pružatelja usluge ako se tražena datoteka nalazi na tom udaljenom pružatelju usluge



1. Korisnik pružatelja usluge SP1 zatraži datoteku. Korisnik odabire datoteku tako što mu SP1 ponudi popis svih dostupnih datoteka, a korisnik onda odabire koju želi. Popis datoteka koje ponudi korisniku, pružatelj usluge prethodno dohvati iz središnjeg registra CR. Na osnovu čega korisnik odabire koju datoteku želi nije bitno za sustav (može biti prema opisu datoteke, imenu datoteke ili nešto treće).
2. Pružatelj usluge prema listama koje je prethodno dohvatio iz središnjeg registra zna gdje se nalazi datoteka (recimo na SP2) i šalje zahtjev za udaljenom datotekom pružatelju usluga SP2. U zahtjevu se nalaze barem sljedeći podaci: ID pružatelja usluge SP1, ID korisnika koji je zatražio datoteku i ID zatražene datoteke. Poruka je kriptirana privatnim ključem SP1.
3. Pružatelj usluge SP2 prima zahtjev, otvara poruku javnim ključem SP1 kojeg je dobio iz certifikata prethodno pribavljenog od SP1 (podsustav za uspostavu infrastrukture javnog ključa). Pružatelj usluge SP2 dohvaća datoteku iz svog lokalnog spremišta i šalje ju zajedno sa podacima: ID pružatelja usluge SP2, ID korisnika koji je zatražio datoteku i ID zatražene datoteke. Poruka je kriptirana privatnim ključem SP2.
4. Pružatelj usluge SP1 prima poruku, otvara ju javnim ključem SP2 kojeg je dobio iz certifikata prethodno pribavljenog od SP1 (podsustav za uspostavu infrastrukture javnog ključa). Zatraženu datoteku prikazuje korisniku (ili mu je pruža preko downloada).