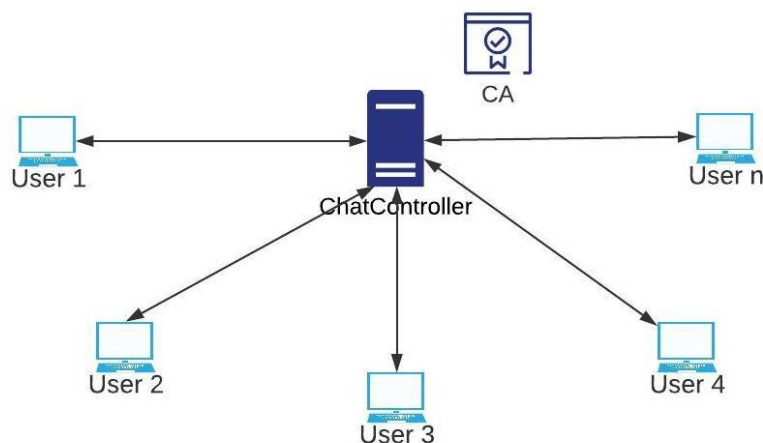


## Zadatak

Implementirati sistem za sigurnu razmjenu poruka između više korisnika. Sistem je prikazan na slici 1. Korisnik se prijavljuje na sistem pomoću višefaktorske autentikacije koja uključuje korisničko ime i lozinku, digitalni sertifikat i token. Sva komunikacija se obavlja posredstvom *ChatController*-a, komponente zadužene za uspostavljanje, praćenje i održavanje sesije između korisnika.

Nakon unosa kredencijala, korisnik prikazuje *ChatController*-u svoj digitalni sertifikat. Nakon provjere sertifikata, *ChatController* šalje korisniku na mail jedinstveni token, koji korisnik unosi u posljednjem koraku autentikacije. Nakon uspješne prijave, korisnik vidi spisak prijavljenih korisnika i može da započne razmjenjivati poruke sa više korisnika istovremeno.



Slika 1. Sistem za razmjenu poruka

*ChatController* se sastoji od sljedećih komponentata koje mogu biti fizički/logički razdvojene, a mogu biti i dio jedne cjeline:

1. komponenta za upravljanje autentikacijom korisnika,
2. komponenta za upravljanje sesijom između korisnika,
3. komponenta za praćenje i detekciju sigurnosno-osjetljivih poruka,
4. komponenta za izdavanje i praćenje izdatih digitalnih sertifikata.

Sistem je potrebno implementirati tako da sva komunikacija bude zaštićena. Prilikom uspostavljanja komunikacije, potrebno je zahtijevati obostranu autentikaciju između korisnika i *ChatController*-a. Svi korišteni digitalni sertifikati treba da budu izdati od strane istog CA tijela, tj. komponente br. 4.

Komponenta za praćenje i detekciju sigurnosno-osjetljivih poruka treba da detektuje svaku poruku čiji sadržaj može da se tretira kao pokušaj napada (SQLInjection, XSS, Parameter Tampering, DoS i sl.). U takvoj situaciji, automatski se terminira sesija između

datih korisnika i oni dobijaju odgovarajuće obavještenje putem istog komunikacionog kanala.

Sve detalje zadatka koji nisu precizno specifikovani realizovati na proizvoljan način. Aplikacije treba da imaju minimalne funkcionalnosti koje su dovoljne za prezentaciju i testiranje rada sistema za razmjenu poruka. Dozvoljena je upotreba proizvoljnog programskog jezika, kao i proizvoljnih tehnologija neophodnih za realizaciju tehničkih detalja. Za potrebe demonstracije, neophodno je da korisnici koji razmjenjuju poruke, kao i *ChatController*, budu na fizički ili logički razdvojenim mašinama (dozvoljena je upotreba virtuelnih mašina, kao i privatnih mreža na nivou virtuelnih mašina).

Studenti koji uspješno odbrane projektni zadatak stiču pravo izlaska na usmeni dio ispita. Na odbranu je potrebno donijeti kompletan izvorni kod projektnog zadatka. Projektni zadatak važi od prvog termina januarsko-februarskog ispitnog roka 2021. godine i vrijedi do objavljivanja sljedećeg projektnog zadatka.