Informaciona bezbednost - projekat

Opis zadatka

Zadatak obuhvata izradu dve aplikacije koje bi trebalo da omoguće sigurnu razmenu e-mail poruka. Sigurnost podrazumeva poverljivost, integritet i neporecivost poruka. Pomenute aplikacije su:

- Web aplikacija, koja služi za distribuciju sertifikata;
- E-mail klijentska aplikacija, koja bi trebala pomoću kriptografskih primitiva da osigura sigurnost e-mail poruke.

Web aplikacija

Web aplikacija koja služi za distribuciju sertifikata bi trebalo da bude izrađena uz pomoć Spring Boot frejmvorka. Uz projektni zadatak dolazi i osnova aplikacije sa svim potrebnim zavisnostima. Aplikacija od entiteta obuhvata:

Entitet User, koji je opisan sledećim atributima:

- Id - celobrojna (autoincrement) vrednost;
- E-mail - tekstualna vrednost;
- Password - tekstualna vrednost, koja se čuva u hešovanom obliku;
- Certificate - tekstualna vrednost, koja čuva naziv datoteke sa sertifikatom (koja se smešta u posebno kreirani direktorijum);
- Active - boolean vrednost kojom je naznačeno da li je korisnikov nalog aktiviran;
- Authority - veza ka entitetu Authority.

Entitet Authority, koji nasleđuje GrantedAuthority, i opisan je sledećim atributima:

- Id - celobrojna (autoincrement) vrednost;
- Name - tekstualna vrednost.

Potrebno je realizovati web aplikaciju da omogući sledeće funkcionalnosti:

- Kreiranje novih korisničkih naloga, pri čemu se novom korisniku dodeljuje Authority tipa *Regular*.
- Odobravanje novih korisničkih naloga od strane administratora;
- Kreiranje korisničkih JKS datoteka - svaki korisnik, nakon što kreira svoj nalog, može da preuzme JKS datoteku koja sadrži:
  - Privatni ključ korisnika i njemu odgovarajući sertifikat;
  - **Za ocenu 10,** taj sertifikat je potpisan od strane CA sertifikata.
- Pretragu korisnika po e-mail-u;
- Preuzimanje sertifikata proizvoljnog korisnika.

Potrebno je obezbediti da se komunikacija sa web aplikacijom odbija putem HTTPS protokola. Pomoću inicijalizacione SQL datoteke je dovoljno dodati Authority za *Admin* i *Regular* tipove korisnika, i inicijalnog administratora.

Klijentska e-mail aplikacija

Okvir klijentske e-mail aplikacije dolazi uz projekat. Kada korisnik sa web aplikacije preuzme svoj JKS file, smešta ga u data folder klijentske aplikacije.

Kako bi Korisnik A i Korisnik B mogli sigurno da razmenjuju e-mailove, potrebno je da sa web aplikacije preuzmu sertifikate jedan od drugoga, i da ih smeste u svoje JKS datoteke pomoću alata ***Portecle***.

Oni tada mogu da razmenjuju e-mailove, u obliku XML poruka sa sledećim elementima:

- Subject - tema e-mail-a u tekstualnom obliku;
- Body - sadržina e-mail-a u tekstualnom obliku.

Komunikacija učesnika

Komunikacija izmedju dva učesnika potrebno je realizovati kroz dva programa (*Writer* i *Reader* klase mail klijenta):

Prvi program šalje poruku:
1. Korisnik A kreira poruku za korisnika B.
2. Korisnik A potpisuje poruku svojim privatnim ključem.
3. Korisnik A šifruje poruku simetričnim ključem i taj simetrični ključ sifruje javnim ključem korisnika B i smešta u poruku.
4. Korisnik A šalje poruku.

Drugi program prima poruku:
1. Asinhrono, korisnik B preuzima poruku sa serverske strane.
2. Korisnik B dešifruje poruku svojim privatnim ključem.
3. Korisnik B verifikuje digitalni potpis poruke pomoću sertifikata korisnika A.
4. Korisnik B čita poruku korisnika A.

Pri šifrovanju i potpisivanju poruke, potpisuje se i šifruje čitava poruka.
Šiforvanjem se postiže da iako svi mogu da vide sve šifrovane poruke, samo ciljani primalac može da je dešifruje. Potpisivanjem se postiže da integritet poruke, primalac se osigurava da poruka nije menjana i neporecivost poruke, da niko drugi do navedeni pošiljalac nije poslao poruku. U suprotnom, digitalni potpis neće odgovarati poruci i sertifikatu.

Algoritmi

Pri šifrovanju se koristi KEK (Key encryption key) metod. Kao algoritam za simetrično šiforvanje koristi se TripleDES. Asimetrični algoritam je RSA.
Pri potpisivanju se korisni enveloped stil. Potpisivanje se vrši pomoću RSA algoritma.

Potrebno je demonstrirati sledeće test slučajeve:

- slanje regularno šifrovane i potpisane poruke
- preuzimanje i prikazivanje regularno šiforvane i potpisane poruke
- detektovanje neregularne poruke sa izmenjenim sadržajem (invalidan potpis)

Za ocene 6, 7 i 8 je dovoljno pomoću Portecle alata odraditi potrebne aktivnosti koje omogućava web aplikacija.
Za ocene 9 i 10 je potrebno odraditi obe aplikacije.