Informaciona bezbednost - projekat 2019

Opis zadatka

Zadatak obuhvata izradu dve aplikacije koje bi trebalo da omoguće sigurno skladištenje slika na serveru. Sigurnost podrazumeva poverljivost, integritet i neporecivost. Pomenute aplikacije su:

- Web aplikacija, koja služi za distribuciju sertifikata i sigurno skladištenje slika;
- Desktop aplikacija, koja bi trebala pomoću kriptografskih primitiva da osigura autentifikaciju prilikom postavljanja slika na server.

Web aplikacija

Web aplikacija koja služi za distribuciju sertifikata bi trebalo da bude izrađena uz pomoć Spring Boot radnog okvira. 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 tako da poseduje 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.
- Upload paketa u kojem se nalaze slike i XML dokument potpisan od strane korisnika.

- Zaštićeno skladištenje, preuzimanje i prikazivanje korisničkih slika.

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

Klijentska (desktop) aplikacija za potpisivanje i pakovanje

Kada korisnik sa web aplikacije preuzme svoj JKS file, smešta ga u data folder klijentske aplikacije.

Potrebno je realizovati desktop aplikaciju tako da poseduje sledeće funkcionalnosti:
- Preuzimanje direktorijuma sa korisničkim slikama za upload
- Kreiranje potpisanog XML-a sa sadržajem opisanim u daljem tekstu
- Paketiranje direktorijuma i pomenutog XML-a u ZIP
- Upload ZIP paketa na server (dodatnih 5 bodova)

XML ima sledeće elemente:
- Korisničko ime korisnika
- Za svaku pojedinačnu sliku:
    - Naziv slike;
    - Veličina slike;
    - Heš slike;
- Datum kreiranja paketa

Algoritmi

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

Nefunkcionalni zahtevi

- Projekat se radi u paru;
- Obavezna upotreba Github platforme (sa kompletnim istorijatom razvoja)
    - Ako koristite privatne repozitorijume, dodati svog asistenta;
- Očekuje se ravnomerna raspodela posla;
- Dozvoljena je upotreba third-party biblioteka za algoritme, zipovanje…