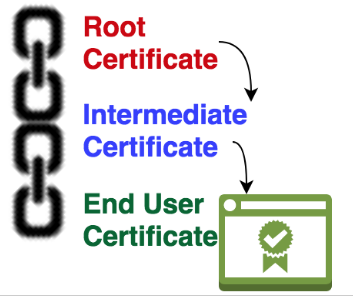
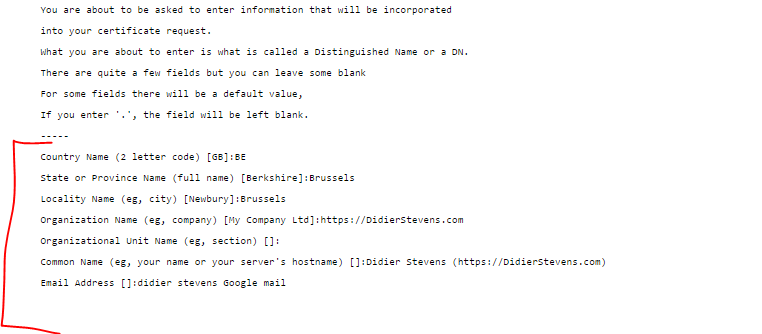
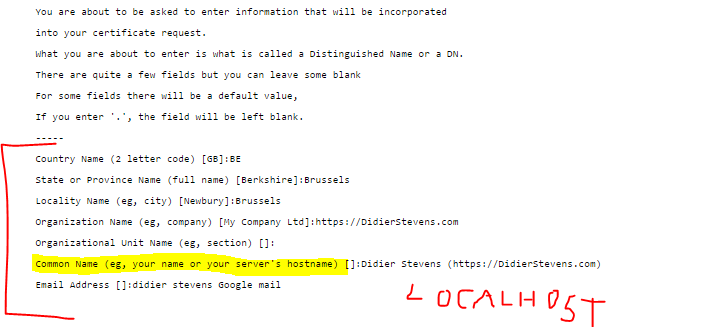
1. Instalira se program za generisanje self signed CA i Intermediate ,Client Certificate link do alata: <https://slproweb.com/products/Win32OpenSSL.html>
2. Zatim pravimo lance sertifikata



1. Jako vazno morate cmd da otvorite u administratorskom rezimu !!! pa tek onda da unosite komande openssl
2. Komande kako se prave sertifikati mozete da vidite ovde <https://blog.didierstevens.com/2008/12/30/howto-make-your-own-cert-with-openssl/>
3. Svi fajlovi koji se koriste bice u folderu https
4. Kada pravite self signed CA sertifikat mozete da izlupate sva polja ovde



1. Taj sef signed CA sto smo napravili dalje koristimo u svim ostalim , kada se pravi neki sertifikata za PKI ,SIEM,FRONT sa self signed CA ga potpisujemo .Jako vazno !!!!!!! svi ovi sertifikati ispod CA moraju da imaju u polju Common name :localhost



1. **Podesavanje server PKI**
2. Pratite ono uputstvo sa komandama za pravljenje sertifikata i dobijemo PKCS12 file koji se kod nas zove keystore.p12 to smestamo u pki/src/main/resources
3. Izmena PKI application.properties dodaju se stvari za https protocol

#https

security.require-ssl=true

# The format used for the keystore

server.ssl.key-store-type=PKCS12

# The path to the keystore containing the certificate

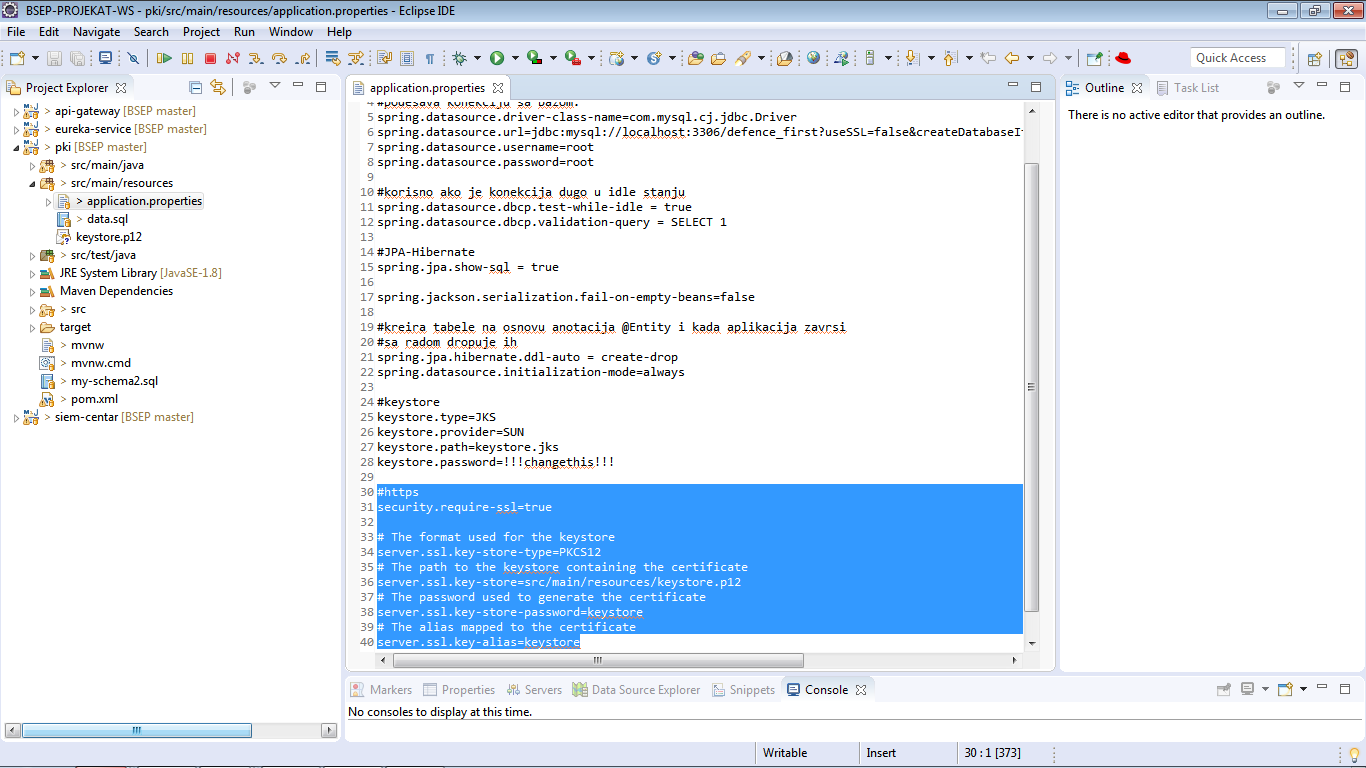
server.ssl.key-store=src/main/resources/keystore.p12

# The password used to generate the certificate

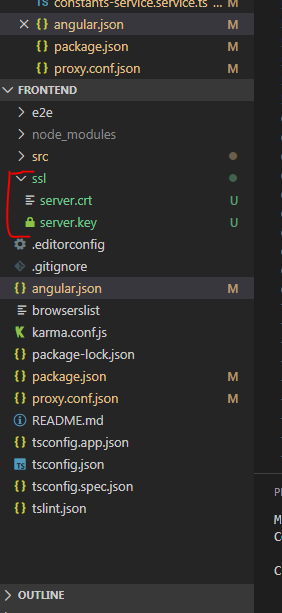
server.ssl.key-store-password=keystore

# The alias mapped to the certificate

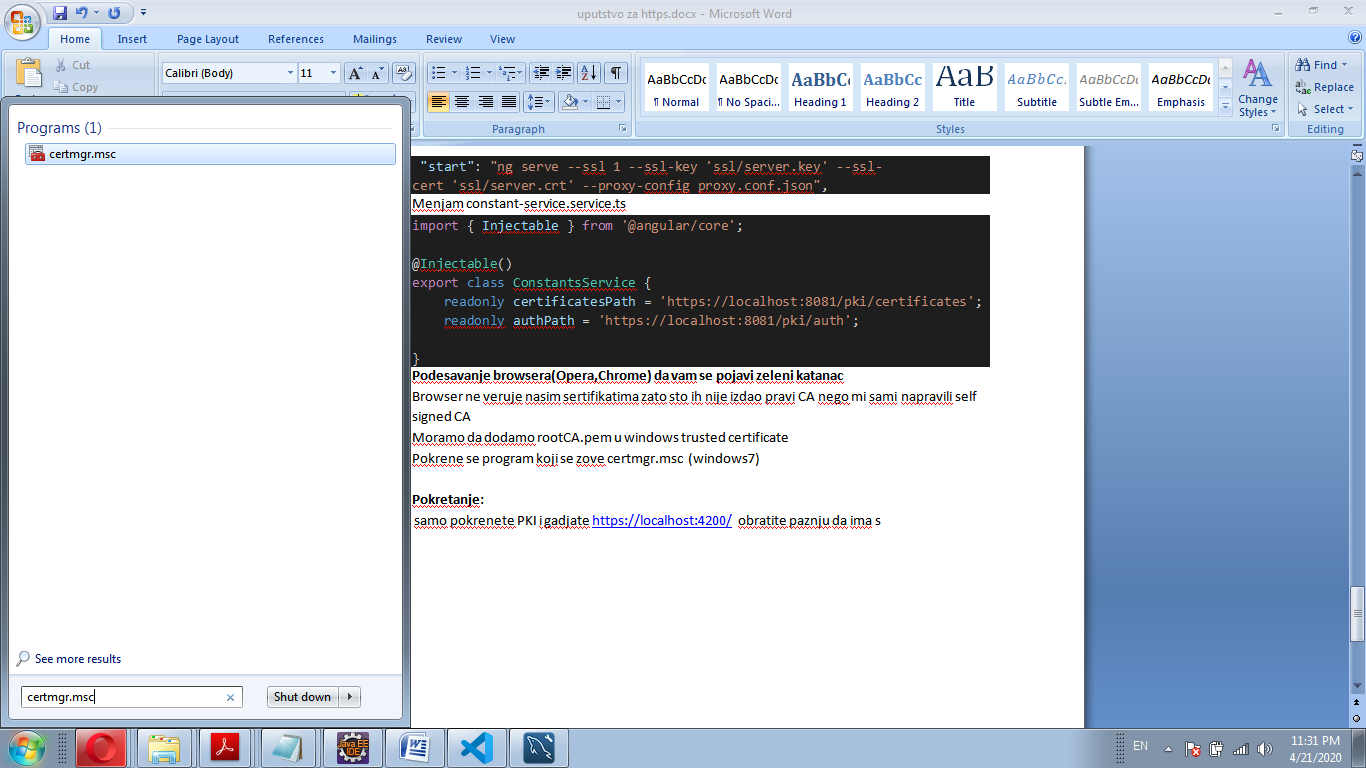
server.ssl.key-alias=keystore



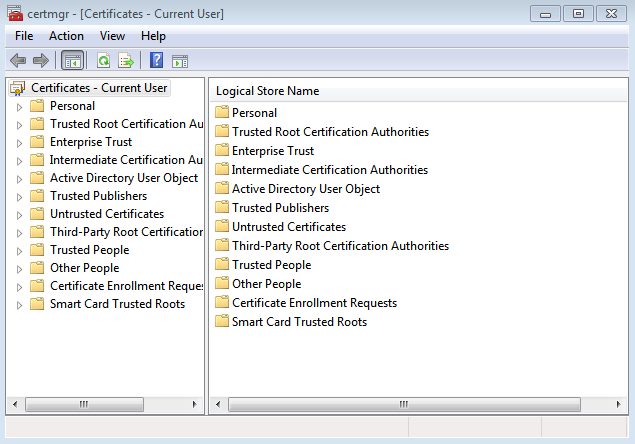
1. **Prelazimo na sredjivanje fronta**
2. prvo napravimo fajlove server.crt i server.key i smestimo ih u folder ssl koji je na nivou src foldera



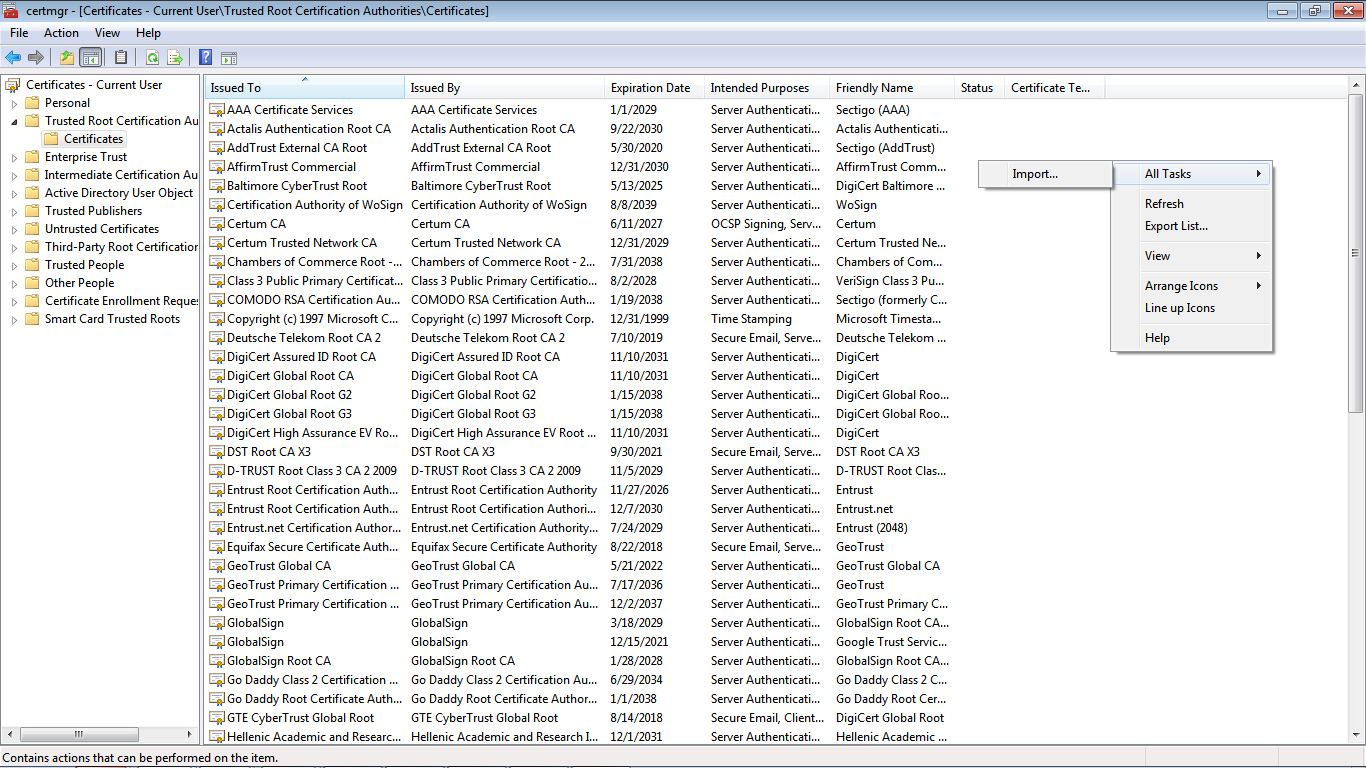
1. Menjam proxy.cong.json(za CORS) prelazim sa http na https
2. {
3. "/pki/\*": {
4. "target": "https://localhost:8081",
5. "secure": true,
6. "logLevel": "debug"
7. }
8. }
9. Menjam angular.json
10. "serve": {
11. "builder": "@angular-devkit/build-angular:dev-server",
12. "options": {
13. "browserTarget": "frontend:build",
14. "proxyConfig": "proxy.conf.json",
15. "ssl":true,
16. "sslCert": "./ssl/server.crt",
17. "sslKey": "./ssl/server.key"
18. },
19. Menjam package.json
20. "start": "ng serve --ssl 1 --ssl-key 'ssl/server.key' --ssl-cert 'ssl/server.crt' --proxy-config proxy.conf.json",
21. Menjam constant-service.service.ts
22. import { Injectable } from '@angular/core';
23. @Injectable()
24. export class ConstantsService {
25. readonly certificatesPath = 'https://localhost:8081/pki/certificates';
26. readonly authPath = 'https://localhost:8081/pki/auth';
27. }
28. **Podesavanje browsera(Opera,Chrome) da vam se pojavi zeleni katanac**
29. Browser ne veruje nasim sertifikatima zato sto ih nije izdao pravi CA nego mi sami napravili self signed CA
30. Moramo da dodamo rootCA.pem u windows trusted certificate
31. Pokrene se program koji se zove certmgr.msc (windows7)



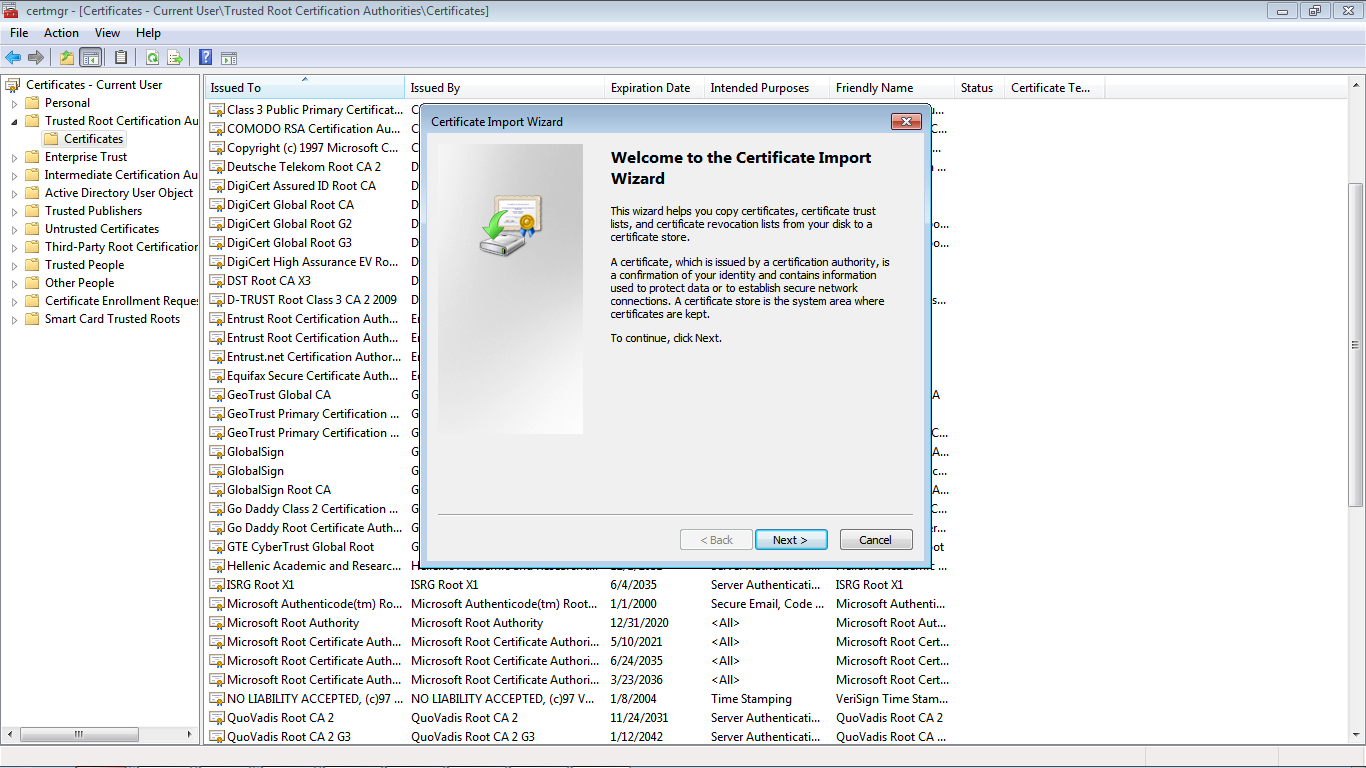
1. Otvara se ovako neki prozor:

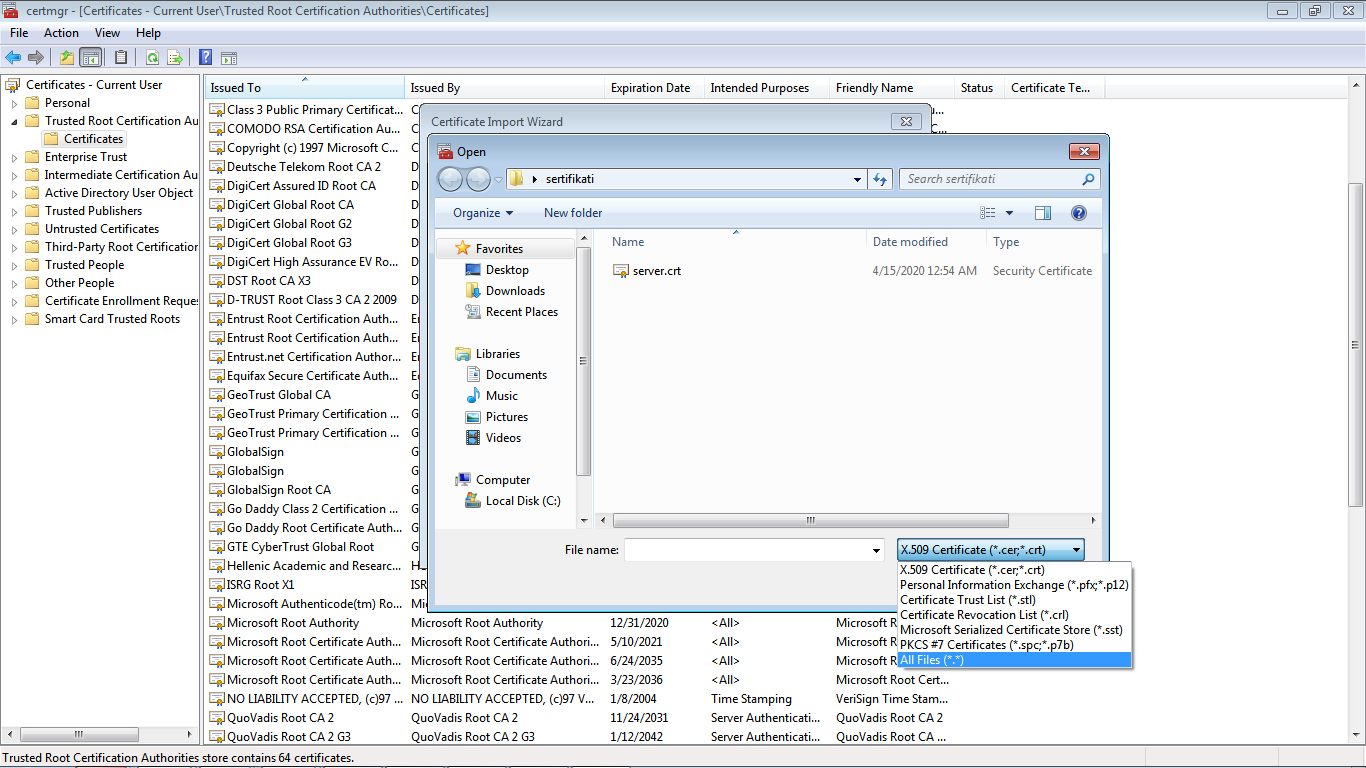


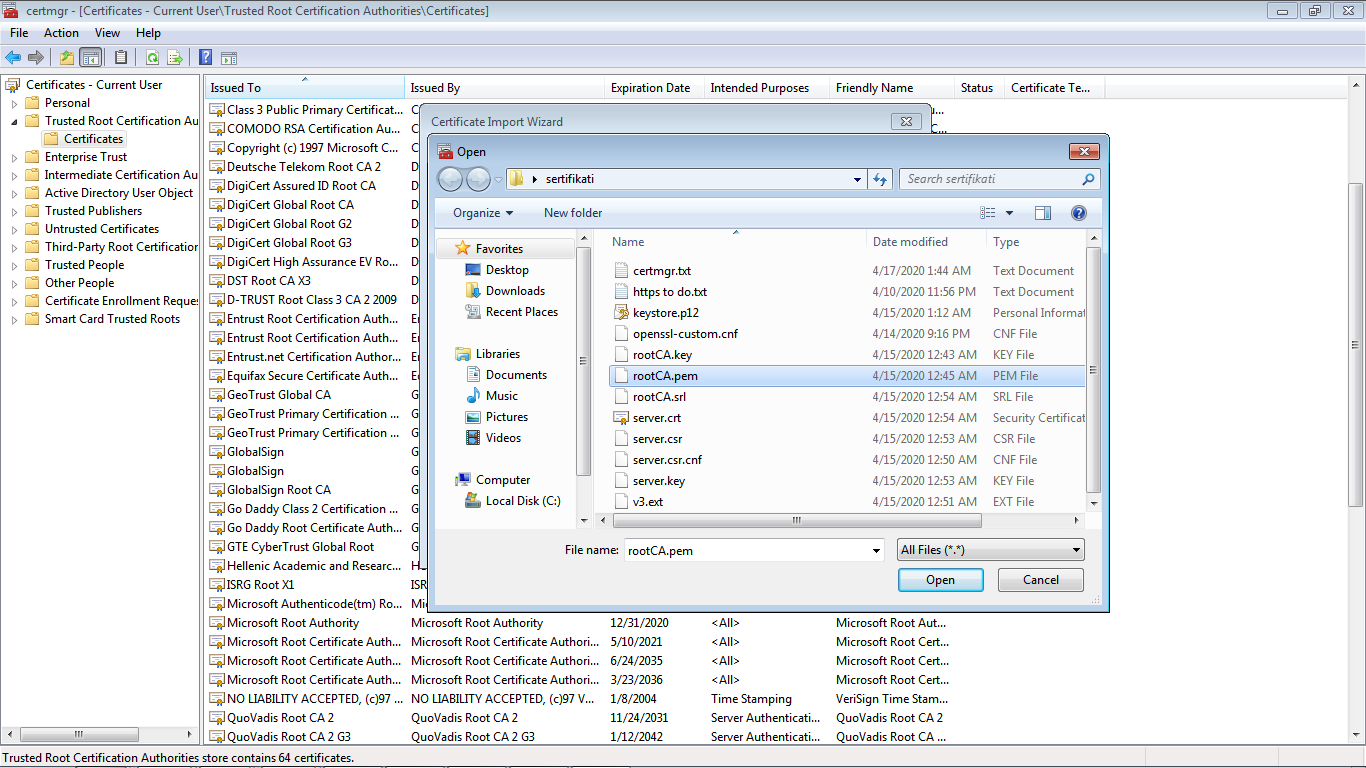
1. Odete na Trusted Root Certification Authorities pa desni klik na belinu i import



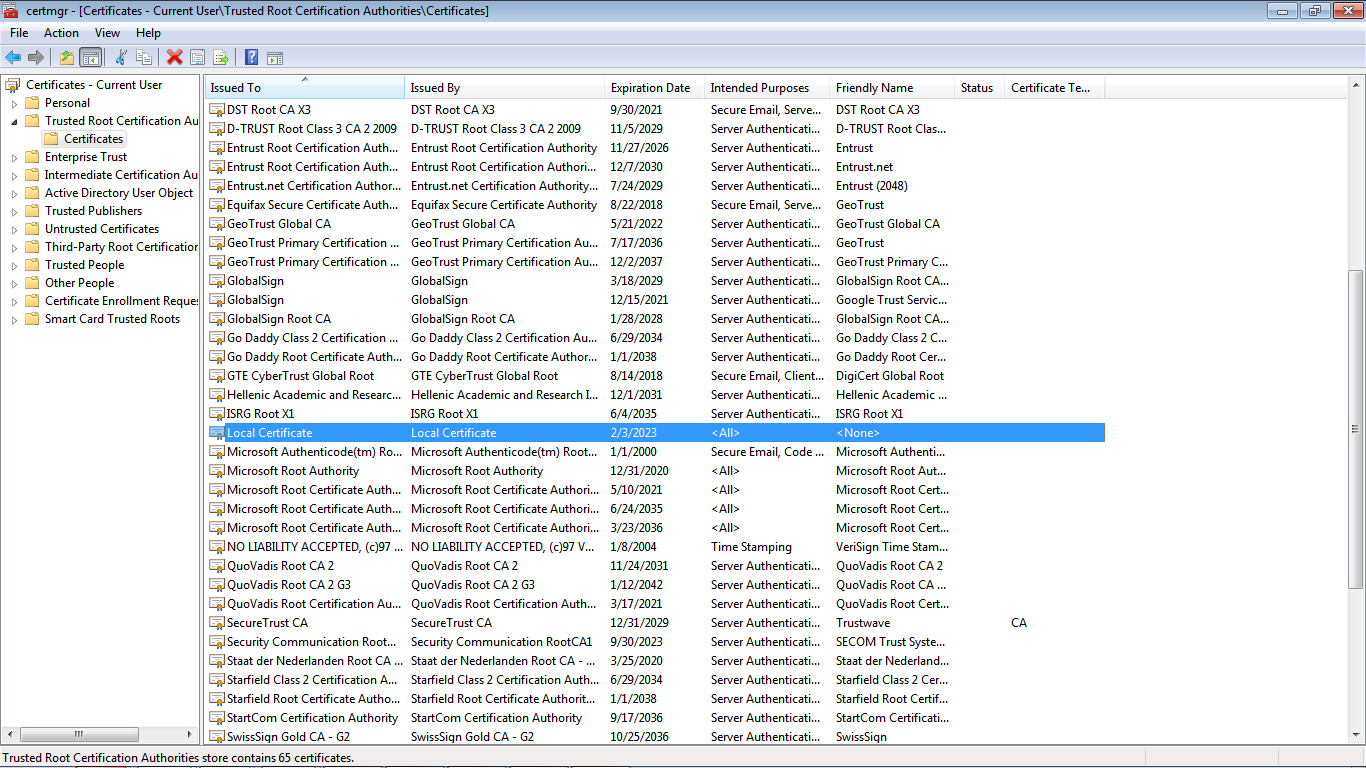
1. Nadjete rootCA.pem i importujte ga







1. Next next next

****

1. Restartujte komp da bi se osvezile promene
2. **Pokretanje:**
3. samo pokrenete PKI i gadjate <https://localhost:4200/> obratite paznju da ima s