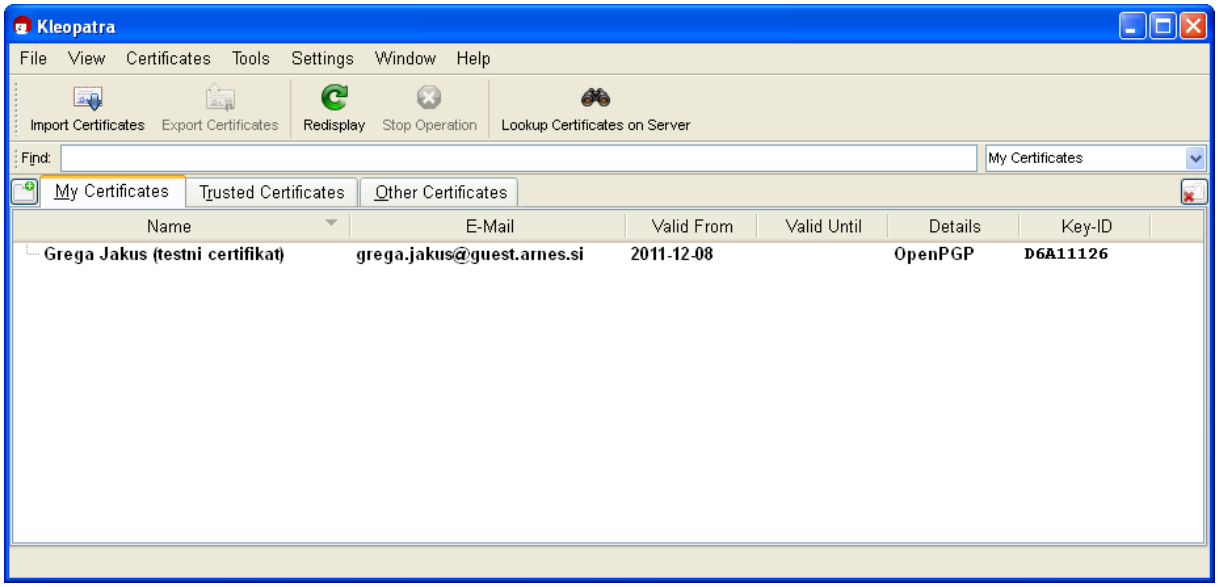
Uporaba asimetričnih šifrirnih postopkov

1) Izdelava para ključev

Z uporabo aplikacije Gpg4win izdelajte par ključev. Uporabite OpenPGP metodo. Sledite 7. poglavju navodil.



2) Shranjevanje ključev

- izvozite **privatni ključ** in ga shranite na varnem mestu (npr. na vašem USB ključku).
- izvozite **javni ključ** in ga poimenujte s svojim imenom in priimkom.

3) Objavljanje javnega ključa

Navadno je potrebno javni ključ objaviti na javnih strežnikih. Ker bomo izdelali javni ključ za testne namene, z njim ne bomo »onesnaževali« javnih strežnikov. Javni ključ bomo zato prenesli na pripravljeno mesto na strežniku.

- S pomočjo spletne aplikacije

http://www.lkn.fe.uni-lj.si/gradiva/Varne_komunikacije/certifikati/upload.html,

prenesite svoj javni ključ na spletno mesto, kjer bo dostopen ostalim.

4) Šifriranje in podpisovanje

- Izberite si 3 sošolce in jim pripravite sporočilo.
- Sporočilo shranite kot tekstovno datoteko, ki jo poimenujete z imenom in priimkom naslovnika (npr. *zaJanezaNovaka*)
- Tekstovno datoteko šifrirajte **z javnim ključem osebe, kateri je sporočilo namenjeno**.
- Tekstovno datoteko podpišite **z vašim privatnim ključem**.
- Tekstovno datoteko prenesite na spletno mesto s pomočjo spletne aplikacije

http://www.lkn.fe.uni-lj.si/gradiva/Varne_komunikacije/certifikati/upload.html

5) Dešifriranje in preverjanje identitete

- Na spletnem mestu

http://www.lkn.fe.uni-lj.si/gradiva/Varne_komunikacije/certifikati/sporocila/

poiščite, če vas čakajo sporočila.

- Prenesite vse datoteke, ki so vam namenjene.
- Vse datoteke dešifrirajte s svojim privatnim ključem in preverite, kdo je njihov pošiljatelj.
- S spletnega mesta prenesite tudi nekaj datotek, ki niso namenjene vam, in jih poskušajte dešifrirati.