

VAJA: Uporaba programa Kleopatra

Namen

Namen naloge je spoznavanje s konceptom strukture javnih ključev in praktično uporabo orodja Kleopatra za upravljanje z digitalnimi identitetami, šifriranjem in dešifriranjem ter digitalnim podpisovanjem dokumentov.

Uvod

V tej nalogi boste raziskali, kako Kleopatra, grafični vmesnik za GnuPG, omogoča enostavno upravljanje s ključi javnega šifriranja. Korak za korakom vas bo vodila skozi procese, kot so ustvarjanje in upravljanje digitalnih certifikatov, šifriranje in dešifriranje dokumentov ter uporaba digitalnih podpisov za zagotavljanje avtentičnosti in integritete dokumentov.

Naloge:

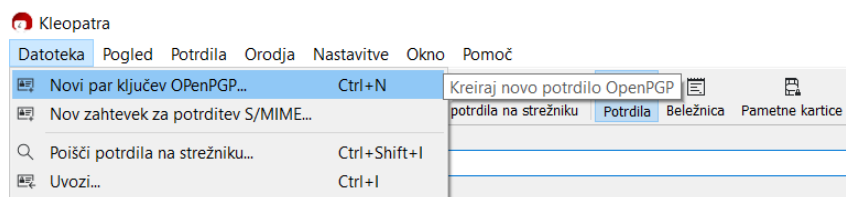
1. Namestitev Kleopatre

Za začetek morate imeti nameščen program Kleopatra. To lahko storite tako, da obiščete spletno stran OpenPGP ([Gpg4win - Download Gpg4win](#)) in prenesete najnovejšo različico za vaš operacijski sistem. Sledite navodilom za namestitev.

2. Izdelava lastnega certifikata

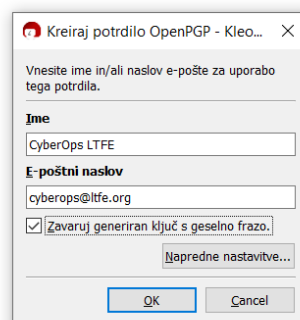
2.1. Zagon kleopatre: Po namestitvi odprite Kleopatro.

2.2. Nov par ključev: V meniju izberite »File« > »New certificate« ali uporabite gumb »New Key Pair«.



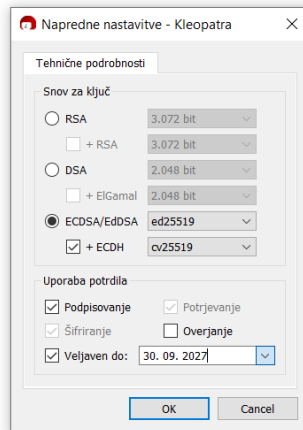
2.3. Izbira tipa ključa: Izberite »Create a personal OpenPGP key pair« in kliknite »Next«.

2.4. Vnos podatkov: Vnesite svoje ime, priimek in e-poštni naslov. Te informacije bodo del vašega certifikata.

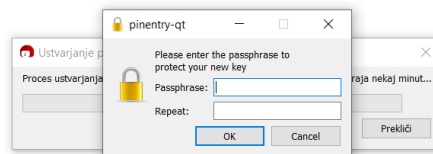


LTFE – Kibernetika varnost

- 2.5. Nadaljnje možnosti: Sledite navodilom za določitev veljavnosti ključa in morebitnih dodatnih e-poštnih naslovov ali psevdonimov.

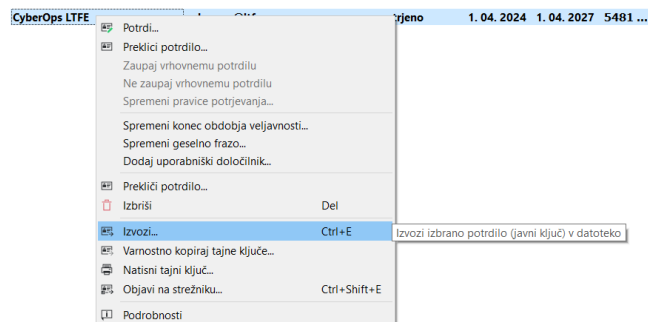


- 2.6. Zaščita ključa: Izberite močno geslo za zaščito vašega zasebnega ključa.



- 2.7. Generiranje ključa: Po končanem vnosu podatkov kliknete »Create Key« in počakajte, da se postopek zaključi.

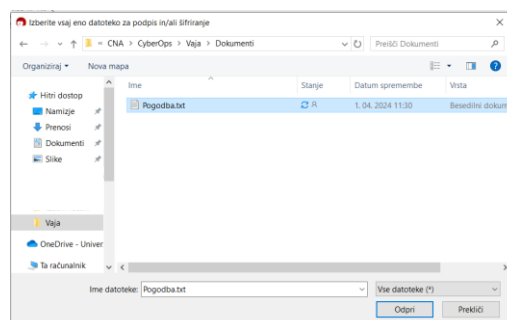
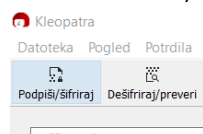
- 2.8. Izvoz javnega ključa: Vaš javni ključ lahko izvozite in delite z drugimi, da vam lahko pošiljajo šifrirana sporočila.



- 2.9. Javni ključ uvozite na SFTP strežnik.

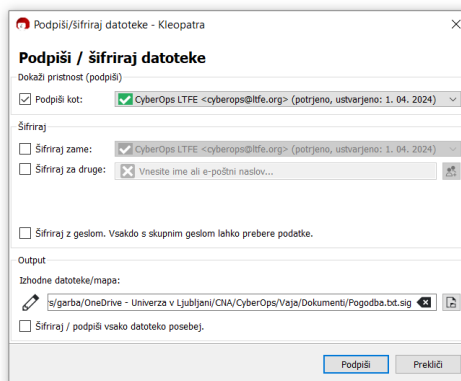
3. Podpisovanje dokumentov

- 3.1. Izbira dokumenta: V kleopatri izberite dokument, ki ga želite digitalno podpisati.



LTFE – Kibernetska varnost

- 3.2. Podpisovanje: Kliknite na »Sing/Encrypt« in izberite »Sign«. Izberite ključ, s katerim želite podpisati dokument.

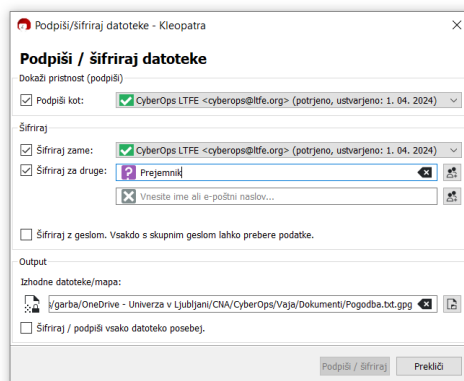


- 3.3. Shranjevanje podpisanega dokumenta: Sledite navodilom za shranjevanje podpisanega dokumenta.

4. Šifriranje dokumentov

- 4.1. Izbira dokumenta: Izberite dokument, ki ga želite šifrirati.

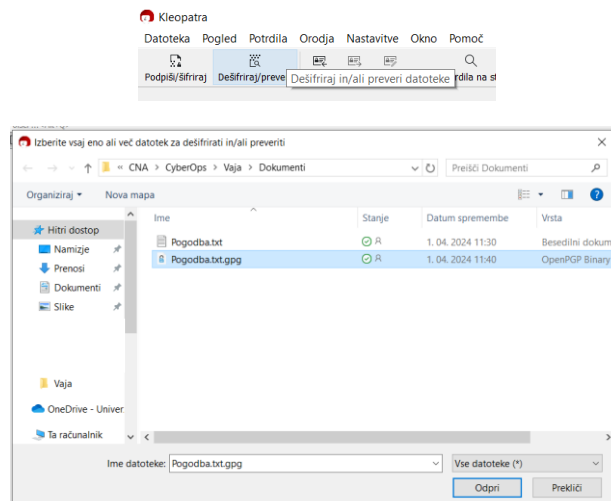
- 4.2. Šifriranje: Kliknite na »Sing/Encrypt« in izberite »Encrypt«. Izberite javni ključ prejemnika, za katerega želite, da lahko dešifrira dokument.



- 4.3. Shranjevanje šifriranega dokumenta: Sledite navodilom za shranjevanje.

5. Dešifriranje dokumentov

- 5.1. Izbira šifriranega dokumenta: Izberite šifriran dokument, ki ga želite dešifrirati.



LTFE – Kibernetetska varnost

5.2. Dešifriranje: Kliknite z desno miško na dokument v kleopatri in izberite »Decrypt/Verify«.

