CARNET

GnuPG i Gpg4win

NCERT-PUBDOC-2018-2-355

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

U današnje vrijeme sve više komunikacije odvija se mrežno, preko Interneta. Takva komunikacija često je nesigurna, a najbolji primjer toga je elektronička pošta čija se razina sigurnosti gotovo uopće nije povisila od 90-tih godina. Upravo zbog tih razloga poželjno je koristiti dodatne alate namijenjene zaštiti komunikacije.

Primjerice, recimo da dvije osobe, Tomislav i Antonio, komuniciraju. Poželjno je da se za njihovu komunikaciju osigura:

- **Tajnost** (eng. *confidentiality)* – nitko osim Tomislava i Antonija ne može pročitati njihove poruke.
- **Vjerodostojnost** (eng. *authenticity*) – mogućnost da Antonio provjeri da poruka zaista dolazi od Tomislava (i obrnuto), a ne od nekoga tko se lažno predstavlja kao Tomislav.

Kako bi se ta svojstva osigurala, razvijeni su razni kriptografski sustavi, standardi i alati. Jedan od najšire korištenih standarda za osiguravanje tajnosti i vjerodostojnosti poruka je OpenPGP. Najpoznatiji slobodni (eng. *free and open source*) alat koji implementira OpenPGP standard je Gnu Privacy Guard (skraćeno GnuPG ili GPG).

Alat GPG moguće je koristiti na operacijskom sustavu Windows kroz programski paket Gpg4win koji između ostaloga sadržava i grafičko sučelje. Ovaj dokument objasnit će kako koristiti GnuPG kroz Gpg4win programski paket, no način uporabe primjenjiv je općenito na GnuPG i ostale alate koji implementiraju OpenPGP standard.

2 Osnove kriptografije javnog i privatnog ključa

Za korištenje GnuPG-a na siguran i ispravan način, potrebno je razumjeti osnove tzv. asimetrične kriptografije. U asimetričnoj kriptografiji svaka osoba koja sudjeluje u komunikaciji ima dva ključa:

- **Javni ključ** koji je poznat svima
- **Privatni ključ** koji mora ostati tajan – svaka osoba mora dobro paziti da nikad nitko drugi ne sazna njen privatni ključ

U ovom poglavlju bit će dan kratki pregled postupka šifriranja i digitalnog potpisivanja pomoću asimetrične kriptografije. Također, bit će opisan problem sigurne razmjene javnog ključa.

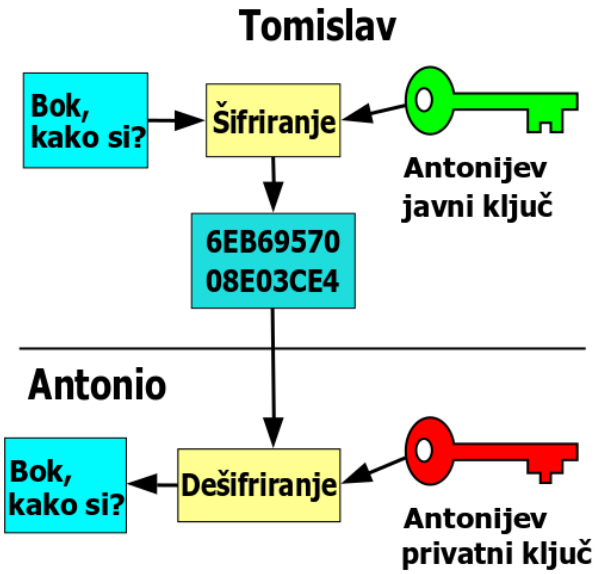
2.1 Šifriranje poruka

Kako bi tajnost komunikacije bila osigurana, potrebno je šifrirati razmijenjene poruke. Najlakše je na primjeru razumjeti kako se asimetričnom kriptografijom šifriraju poruke. Recimo da dvije osobe, Tomislav i Antonio, komuniciraju. Tomislav želi Antoniu poslati poruku „Bok, kako si?“ bez da itko drugi sazna njen sadržaj. Kako bi to postigao, Tomislav tu poruku **šifrira**.

Asimetričnom kriptografijom, Tomislav će to napraviti na sljedeći način:

1. Tomislav nekako pribavi Antonijev javni ključ
2. Zatim, Tomislav napiše poruku „Bok, kako si?“ te ju **šifrira Antonijevim javnim ključem**
3. Tomislav pošalje tu šifriranu poruku Antoniju
4. Antonio primljenu šifriranu poruku **dešifrira svojim privatnim ključem** te ju sada može pročitati

Dijagram na slici Slika 1 vizualno prikazuje postupak šifriranja i dešifriranja poruke iz prethodno navedenog primjera.



Slika 1 –Šifriranje i dešifriranje poruke asimetričnom kriptografijom.

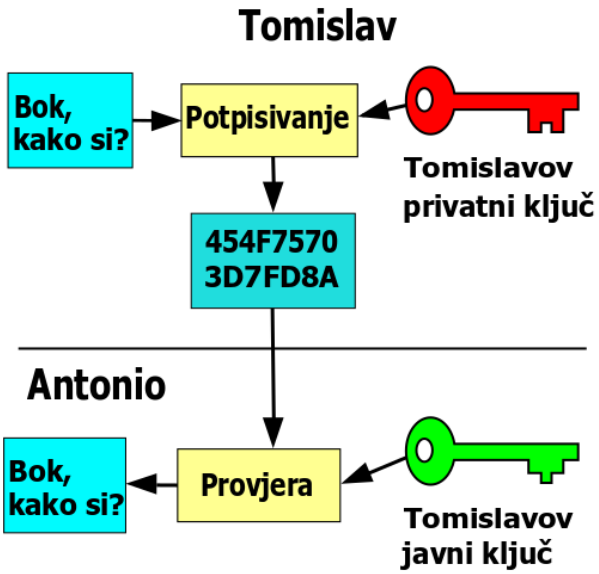
2.2 Digitalno potpisivanje

Šifriranjem poruke riješen je problem tajnosti, no ostaje problem vjerodostojnosti – Antonio želi znati da mu je zaista Tomislav poslao poruku, a ne netko drugi. Kako bi taj problem bio riješen, koristi se postupak digitalnog potpisivanja.

Asimetričnom kriptografijom Tomislav može dokazati da je zaista on poslao poruku na sljedeći način:

1. Tomislav poruku **potpisuje svojim privatnim ključem**
2. Potpisanu poruku Tomislav pošalje Antoniju
3. Antonio pribavi Tomislavov javni ključ
4. Antonio, kao i svatko drugi tko je u posjedu Tomislavovog javnog ključa, sada može **provjeriti ispravnost potpisa Tomislavovim javnim ključem** te tako potvrditi da je zaista Tomislav napisao poruku

Dijagram na slici 2 prikazuje prethodno opisani postupak digitalnog potpisivanja poruke te provjere potpisa.



Slika 2 - Potpisivanje i provjera potpisa poruke asimetričnom kriptografijom

Takvu, digitalnu potpisanu poruku Tomislav može i šifrirati Antonijevim javnim ključem kako bi se u isto vrijeme osigurale i tajnost i vjerodostojnost.

2.3 Problem razmjene ključeva

Kod ovakvog sustava javnih i privatnih ključeva postoji problem sigurne razmjene ključa – kako Antonio zna da zaista ima Tomislavov javni ključ, a ne ključ napadača koji se lažno predstavlja kao Tomislav?

Primjerice, Tomislav je objavio svoj javni ključ na svojoj Web stranici. No, napadač Marko zatim preuzima kontrolu nad tom Web stranicom te mijenja objavljeni Tomislavov ključ svojim ključem. Sada, Antonio s Tomislavove Web stranice preuzima Markov javni ključ misleći da je to zapravo Tomislavov ključ. U konačnici, Marko se može lažno predstaviti kao Tomislav u komunikaciji s Antoniom.

Jednostavno rješenje ovog problema je sigurno uspoređivanje otiska (eng. *fingerprint*) ključa, koji je puno manje duljine nego sam javni ključ. Antonio se može uživo naći s Tomislavom te usporediti otisak javnog ključa kojeg je preuzeo s otiskom Tomislavovog javnog ključa. Ako su otisci isti, Antonio može biti siguran da je ključ kojeg je preuzeo zaista Tomislavov ključ. Alternativno, Antonio se ne mora naći uživo s Tomislavom, već mogu taj postupak obaviti i telefonski ili na bilo koji drugi siguran način. Bitno je da se otisak i javni ključ ne razmjenjuju istim komunikacijskim kanalom.

Postoje i drugi načini rješavanja ovog problema koji su složeniji, no imaju neke svoje prednosti. Jedan način je korištenje tzv. infrastrukture javnog ključa (eng. *Public Key Infrastructure*, skraćeno *PKI*) u kojoj treće strane provjeravaju vlasništvo ključeva te ih potpisuju. Drugi način je decentralizacija povjerenja kroz mrežu povjerenja (eng. *web of trust*). Detaljniji opisi ovih sustava izvan su opsega ovo dokumenta, no korisno je znati da postoje.

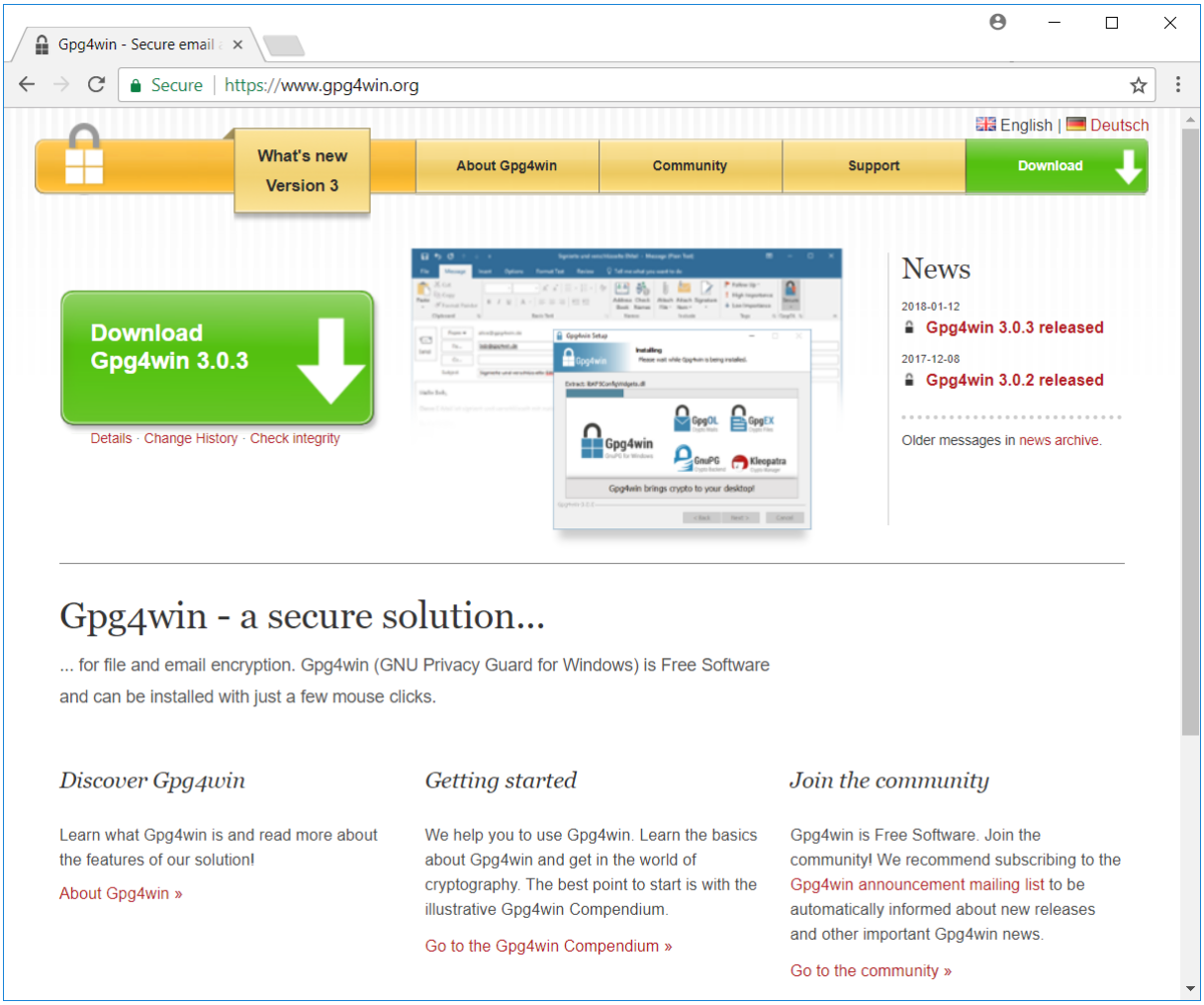
3 Korištenje GnuPG-a kroz Gpg4win sučelje

GnuPG je slobodna (eng. *free and open source*) implementacija standarda OpenPGP koja je nastala kao pandan komercijalnim alatima koji implementiraju taj standard. Najpoznatiji takav komercijalni alat je PGP (skraćeno od eng. *Pretty Good Privacy*), iz kojeg je i nastao OpenPGP standard.

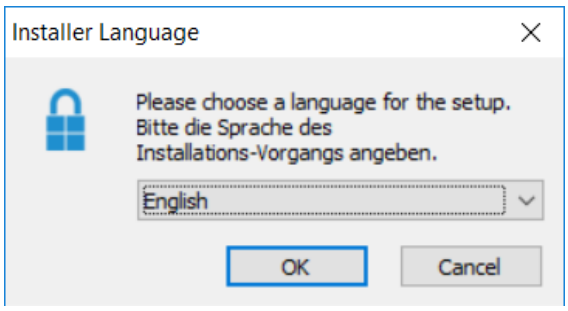
U ovom poglavlju bit će opisan primjer korištenja GnuPG alata na operacijskom sustavu Windows kroz Gpw4win. Gpg4win je skup alata koji uključuje GnuPG i grafičko sučelje za njegovo korištenje.

3.1 Instalacija

1. Za preuzimanje paketa Gpg4win na računalo, potrebno je otvoriti službene stranice alata te pritisnuti na zelenu ***Download*** tipku.

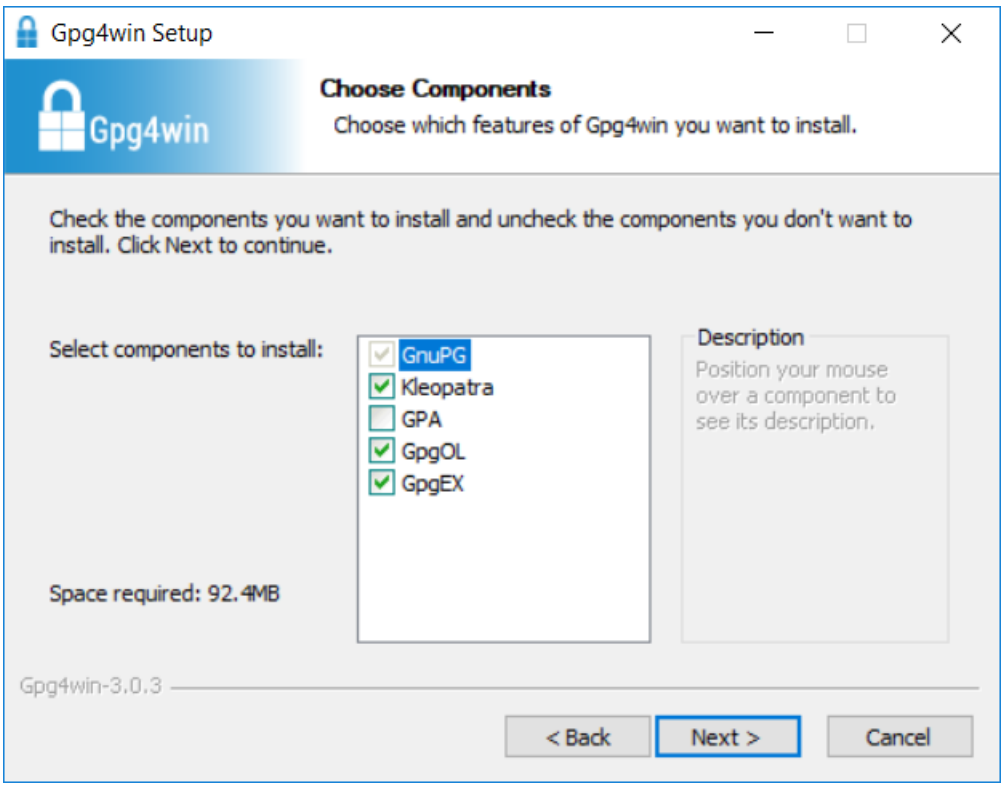


2. Nakon što je datoteka preuzeta i pokrenuta, pojavit će se okvir za odabir jezika. Kako ne postoji prijevod na hrvatski jezik, u ovom dokumentu upute su napisane za engleski jezik. Potrebno je pritisnuti ***OK*** za nastavak instalacijskog procesa.

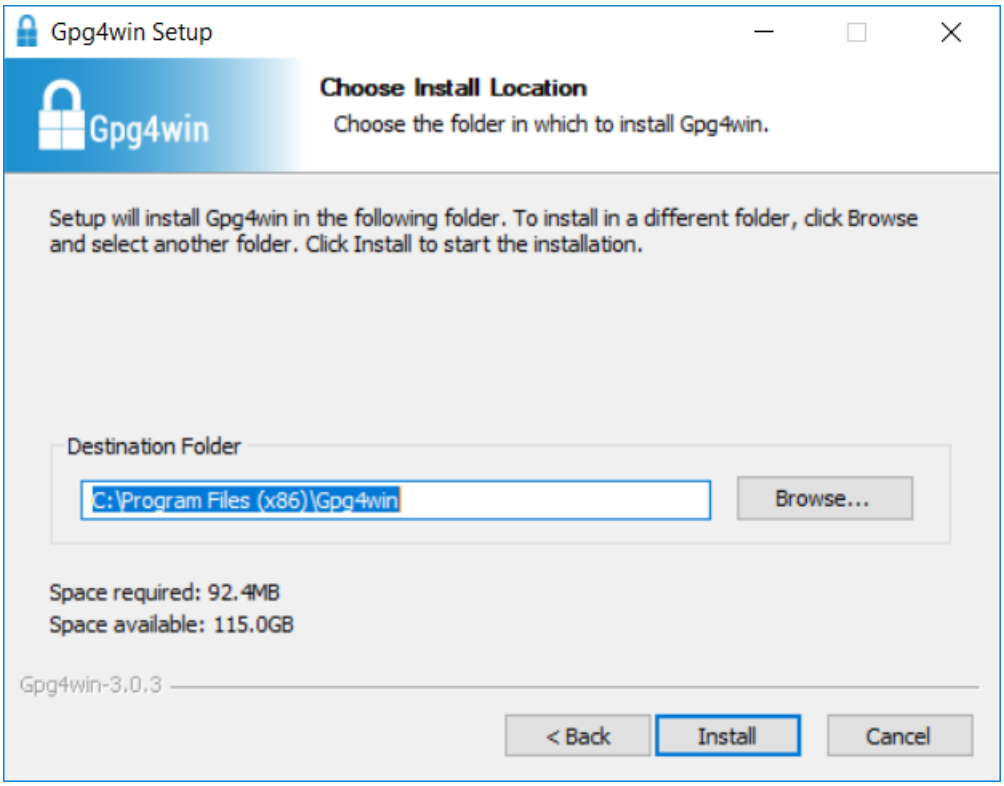


3. Za sljedeći korak potrebno je pritisnuti ***Next***.

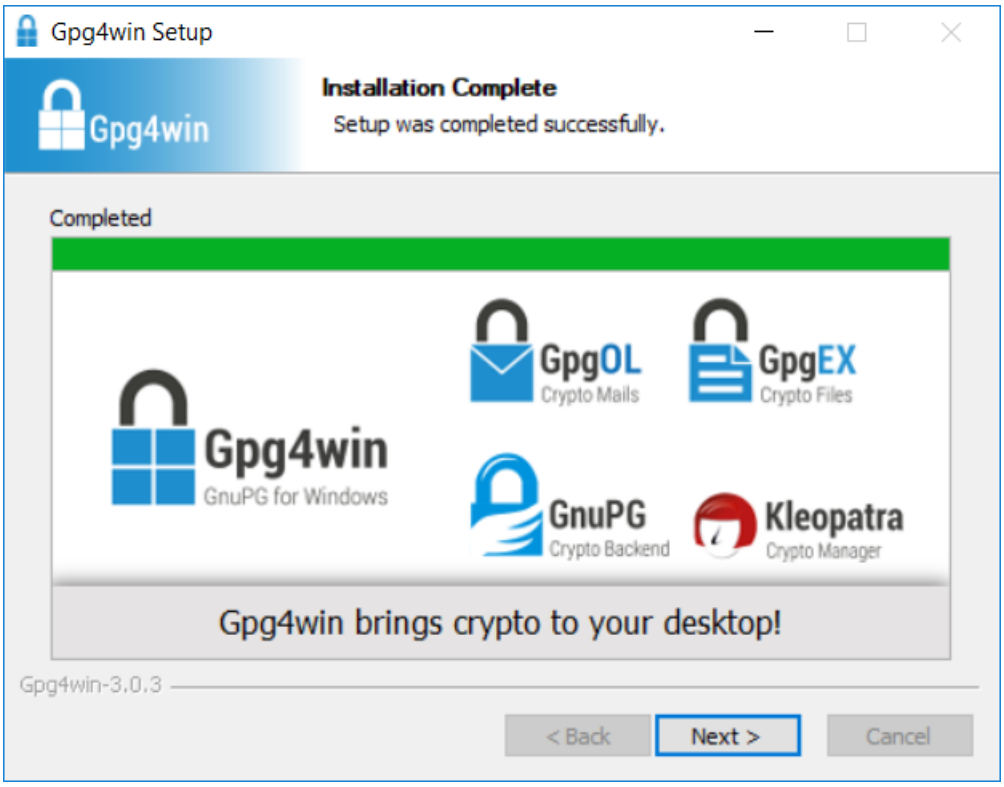
4. U ovom koraku potrebno je odabrati komponente paketa Gpg4win koje će biti instalirane na računalo. Važno je da bude odabran i alat *Kleopatra* koji će se koristiti u nastavku dokumenta. *Kleopatra* je grafičko sučelje i upravlja ključevima.



5. Nakon odabira instalacijskog direktorija, pritiskom na tipku ***Install*** počinje kopiranje datoteka na računalo.



6. Nakon što je instalacija uspješno završena, potrebno je pritisnuti ***Next***.



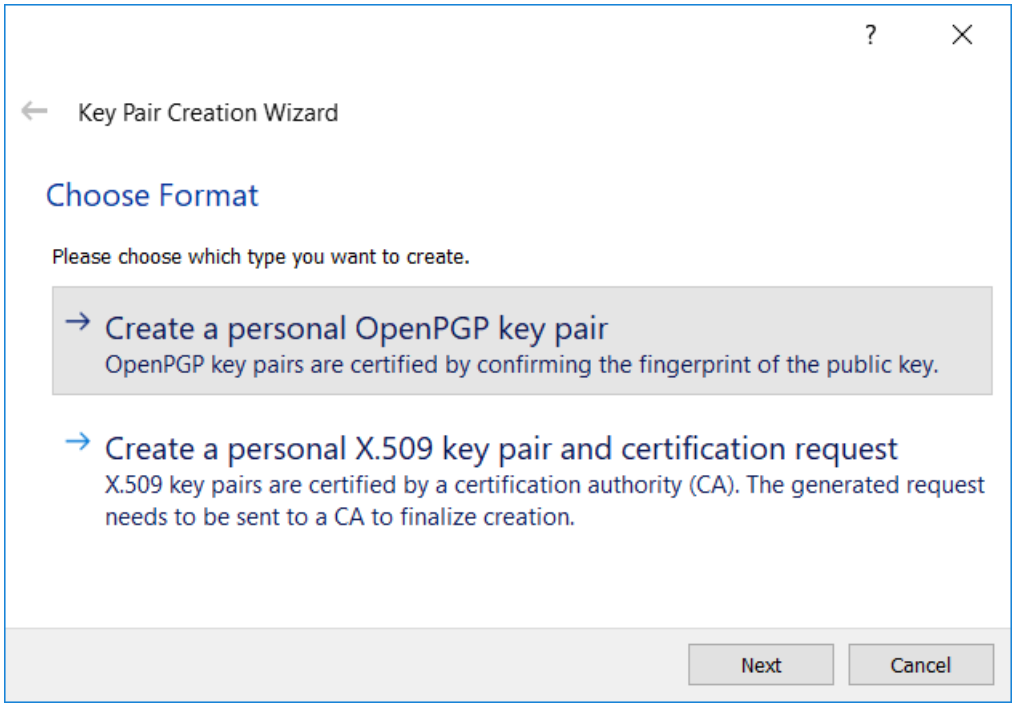
7. Kako bi zatvorili instalacijski program potrebno je pritisnuti ***Finish***.

3.2 Korištenje

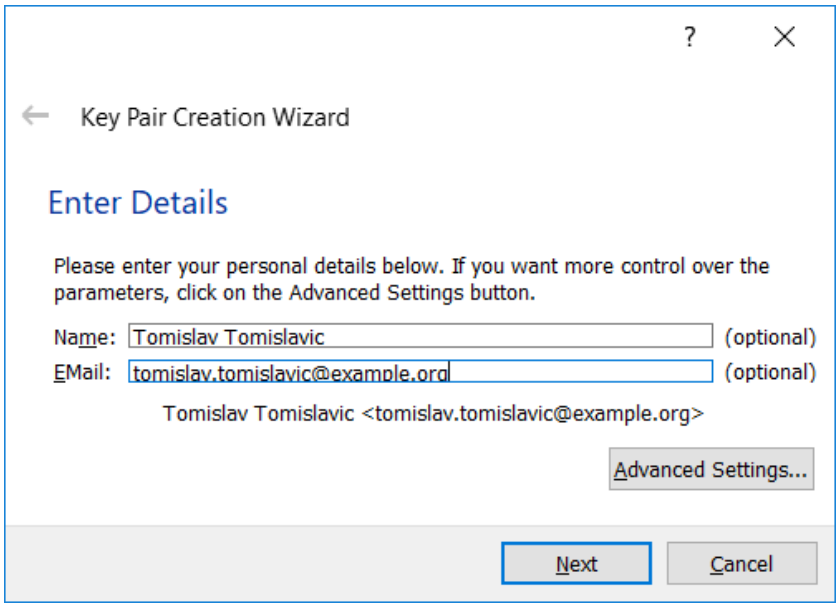
3.2.1 Generiranje javnog i privatnog ključa

Prečac na alat *Kleopatra* može se naći na radnoj površini (eng. *desktop*) računala. Kako na računalu nisu postavljani vlastiti ključevi prvo ih je potrebno generirati. Pritiskom na ikonu s natpisom ***New Key Pair*** otvara se okvir za generiranje ključeva.

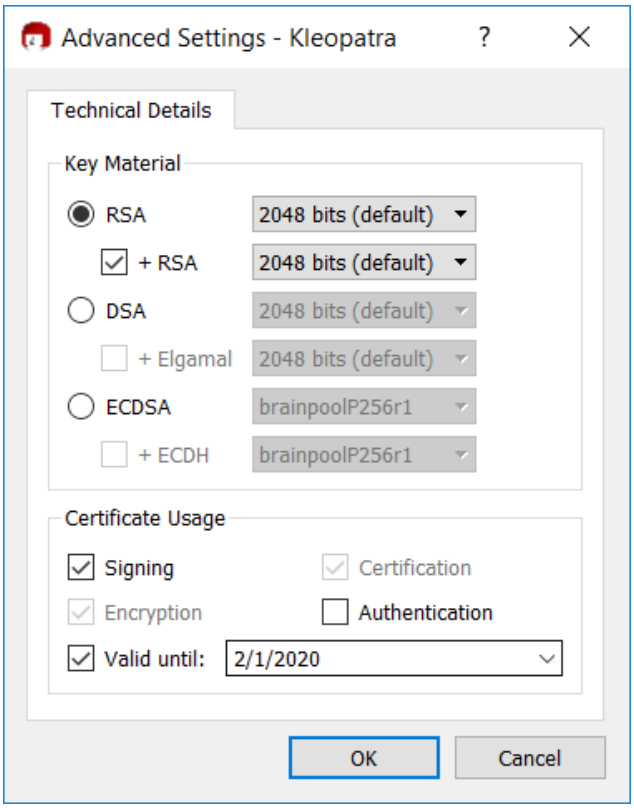
Potrebno je odabrati ***Create a personal OpenPGP key pair***.



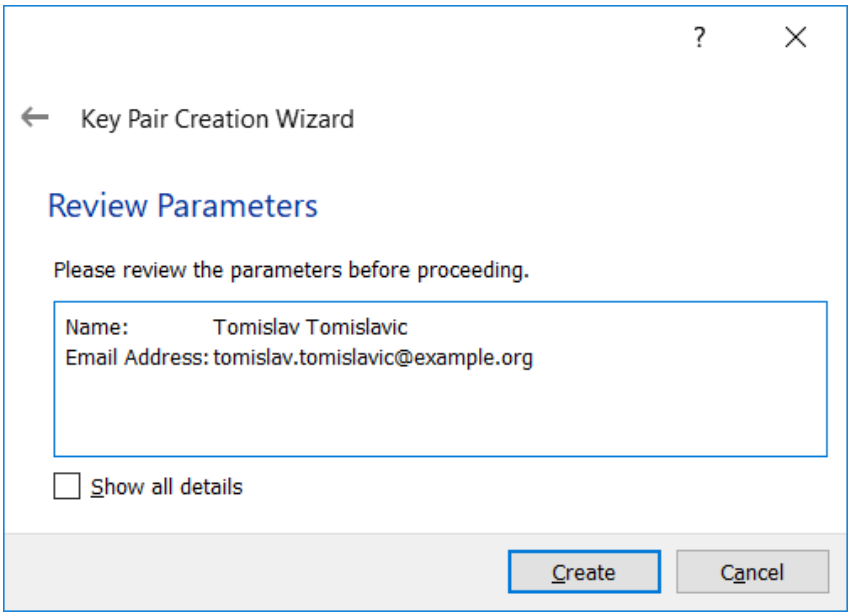
Iako nisu potrebni za rad GPG-a, ime i adresa e-pošte se koriste kako bi se lakše identificirao vlasnik ključa pa ih je svakako poželjno ispravno upisati.



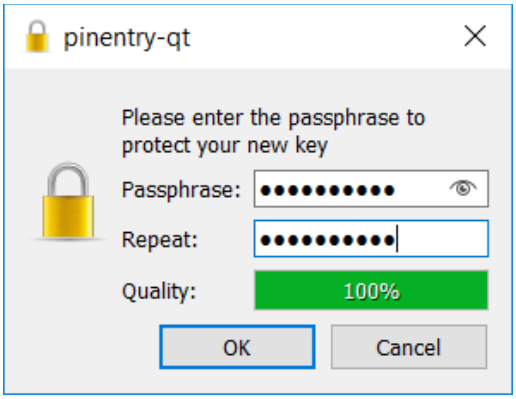
Pritiskom na ***Advanced Settings...*** otvara se prozor u kojem je moguće namjestiti postavke ključeva. Odabrane postavke su većinom sigurne, no kao dobru sigurnosnu mjeru poželjno je postaviti i istek ključa na određeni datum pod *Valid until.* U ovom slučaju odabrano je vrijeme od 2 godine.



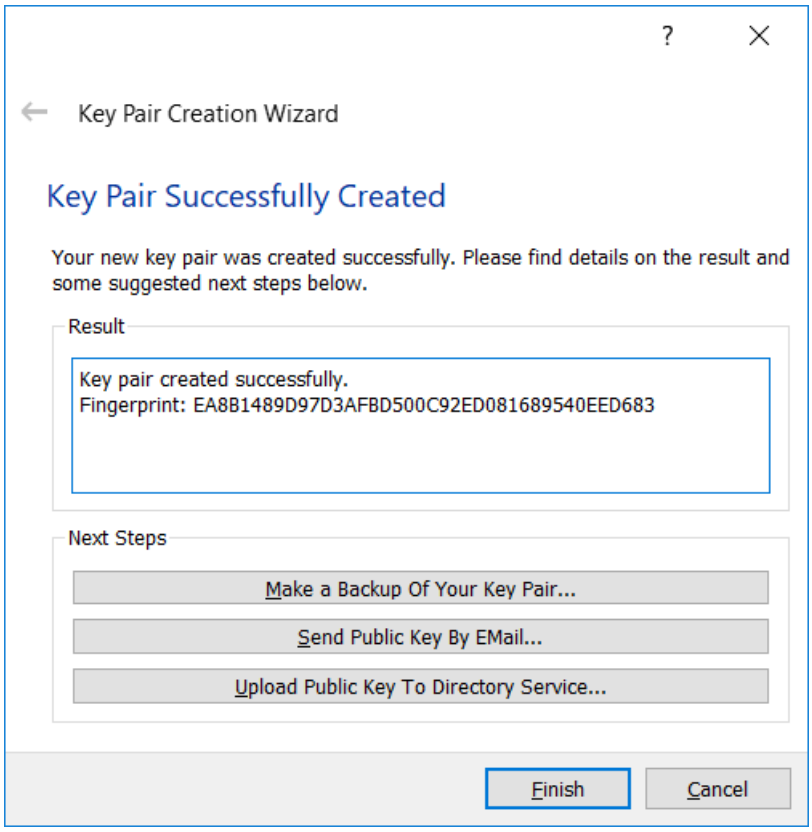
Nakon pritiska na ***OK*** kako bi se potvrdili odabrani detalji certifikata, pritiskom na ***Create*** počinje generiranje certifikata.



Sada je potrebno odabrati lozinku za privatni ključ. Moguć je rad i bez lozinke, no kako je privatni ključ lagano preuzeti s računala korisnika, lozinka predstavlja važnu sigurnosnu mjeru. Nakon potvrde lozinke potrebno je pritisnuti ***OK***.



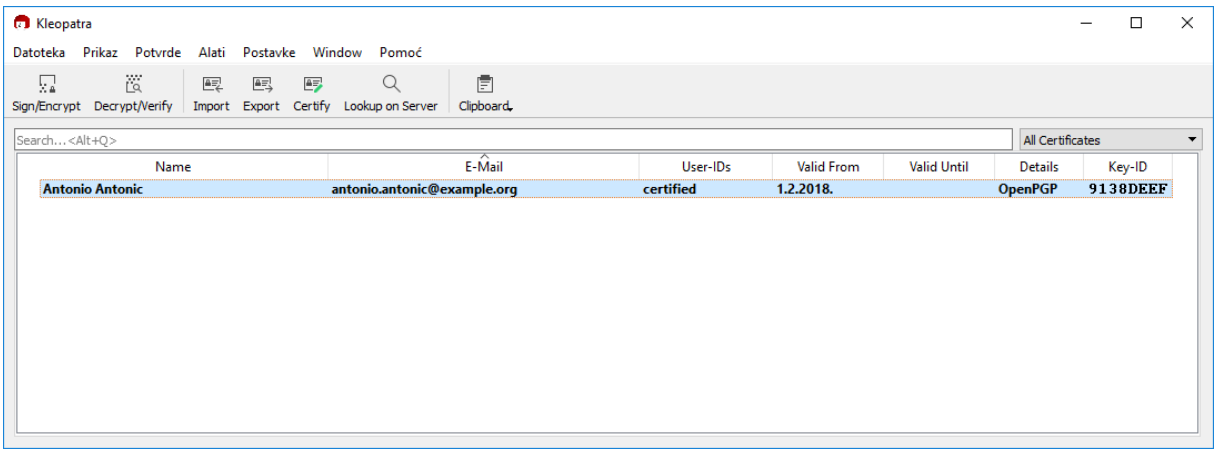
Par javnog i privatnog ključa sada je stvoren. U tekstualnom okviru prikazan je i otisak ključa čija je uloga u sigurnoj razmjeni ključa objašnjena u prethodnom poglavlju.



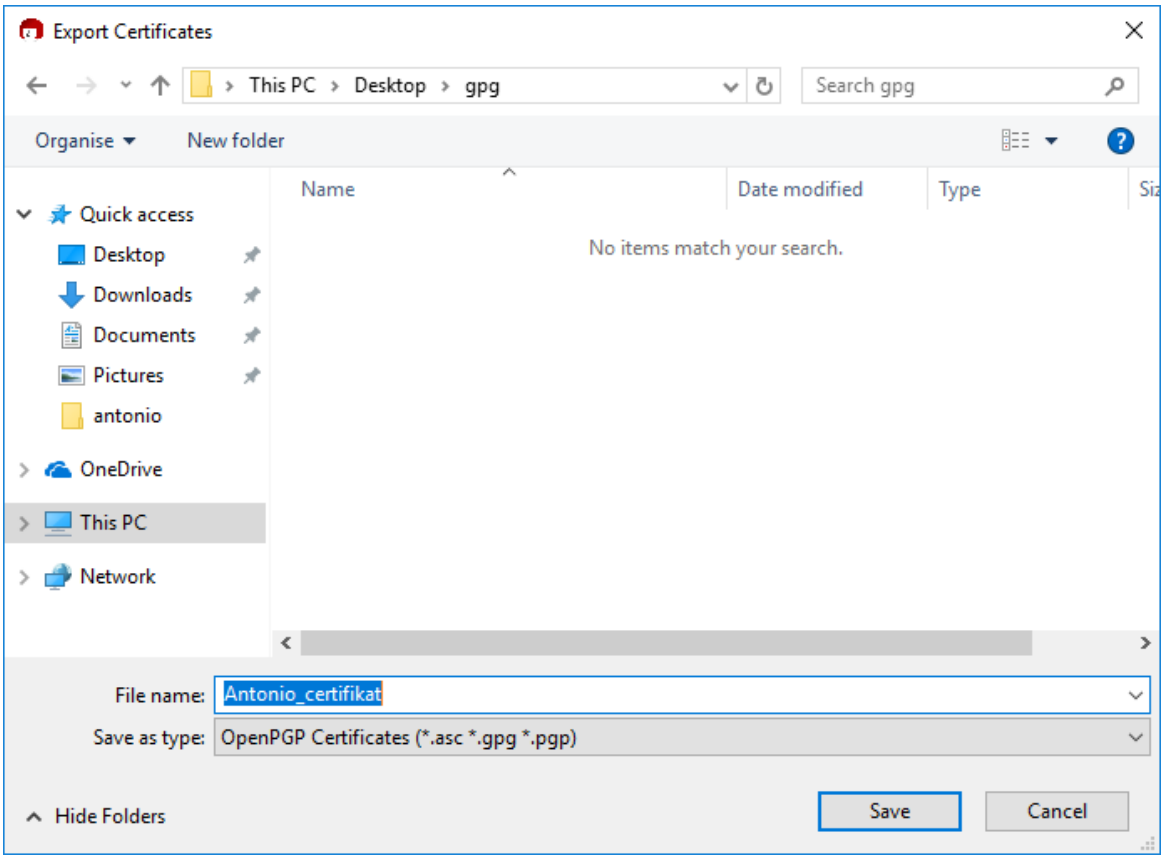
U daljnjim primjerima podrazumijeva se da je istovjetan postupak napravljen i na računalu korisnika *Antonio.*

3.2.2 Izvoz i uvoz javnih ključeva

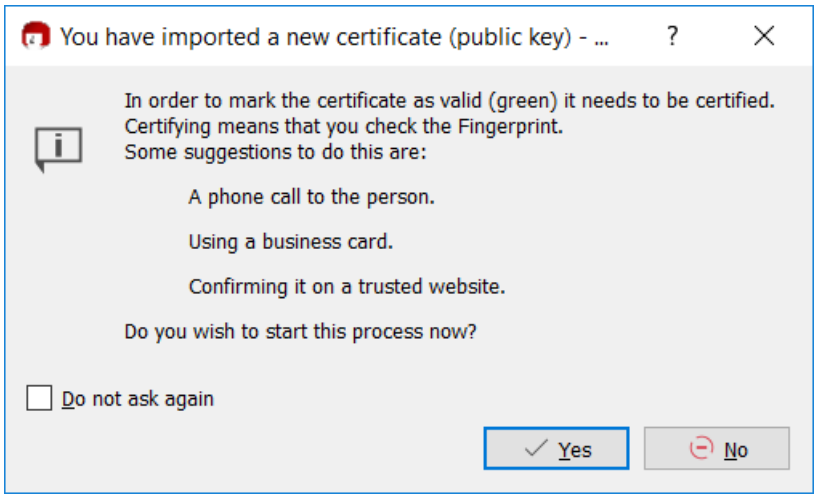
Sada je potrebno dohvatiti i uvesti Antonijev javni ključ u alat *Kleopatra*. To je najlakše napraviti tako da se javni ključ pomoću alata *Kleopatra* izveze (eng. *export*) u datoteku koju će tada Antonio poslati Tomislavu. Na Antonijevom računalu u alatu *Kleopatra* potrebno je označiti Antonijev par ključeva te pritisnuti ikonu s natpisom ***Export.***



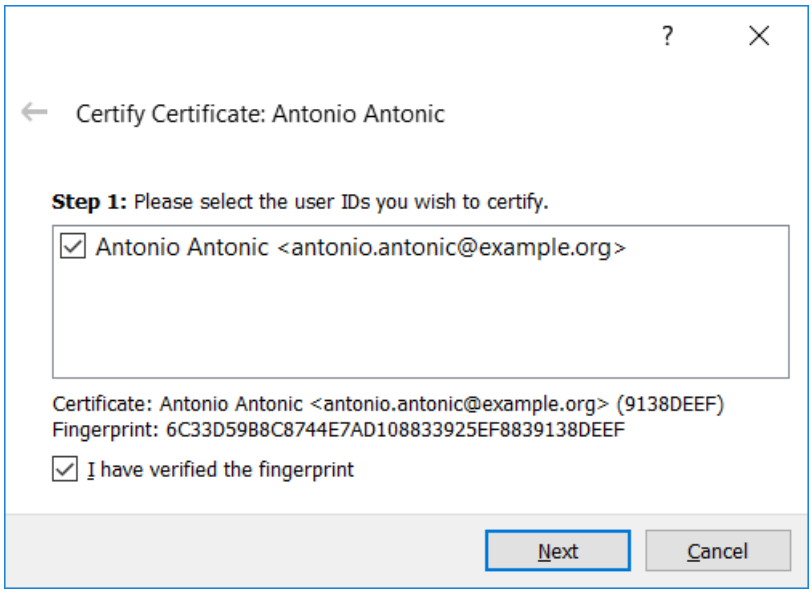
Zatim je potrebno upisati ime datoteke te ju spremiti pritiskom na ***Save***.



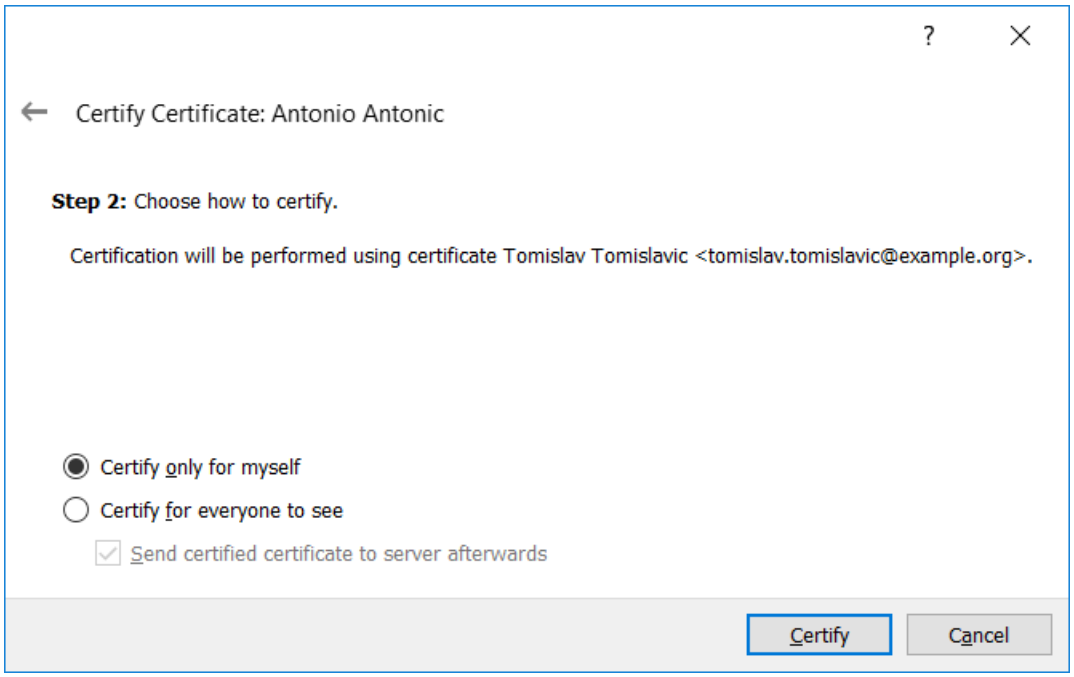
Na Tomislavovom računalu potrebno je uvesti (eng. *import*) Antonijev javni ključ. Dvostrukim pritiskom na datoteku s Antonijevim javnim ključem otvara se prozor u kojem je potrebno potvrditi povezanost javnog ključa s osobom Antonio. Pritiskom na ***OK*** počinje sljedeći korak.



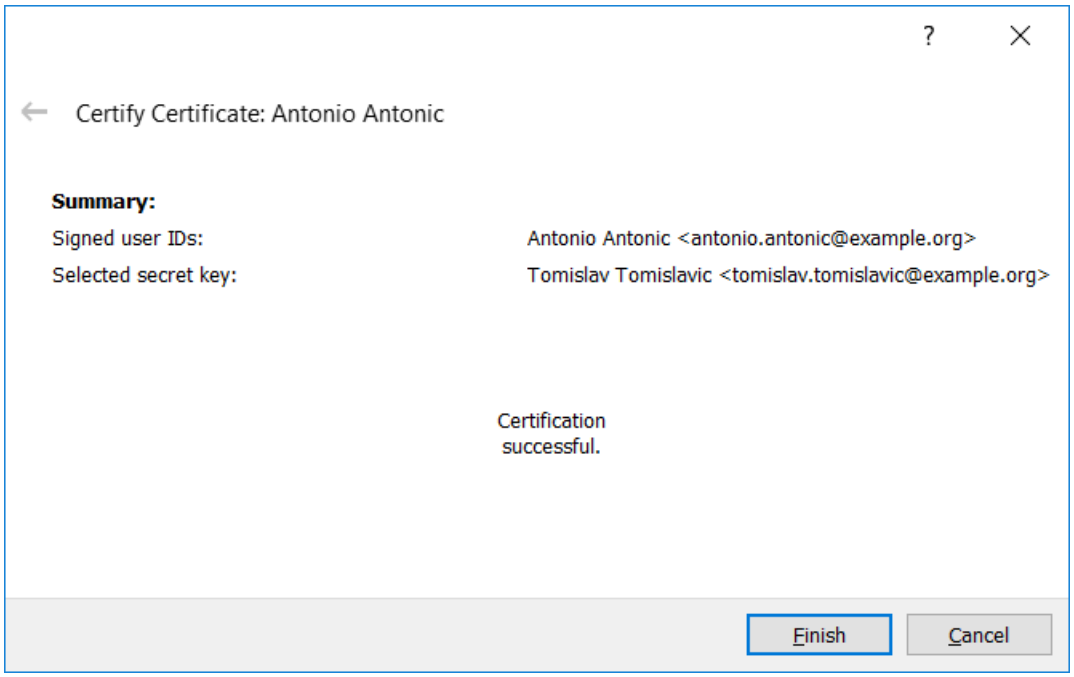
Nakon što je provjerena podudarnost otiska ključa koji je Antonio poslao i koji je Tomislav primio, potrebno je označiti ime korisnika kojeg želimo potvrditi i kućicu uz *I have verified the fingerprint* te pritisnuti na ***Next***.



U sljedećem koraku potrebno je pritisnuti na ***Certify*** kako bi Tomislav svojim privatnim ključem jamčio povezanost javnog ključa i Antonijevih podataka tj. stvorio certifikat.

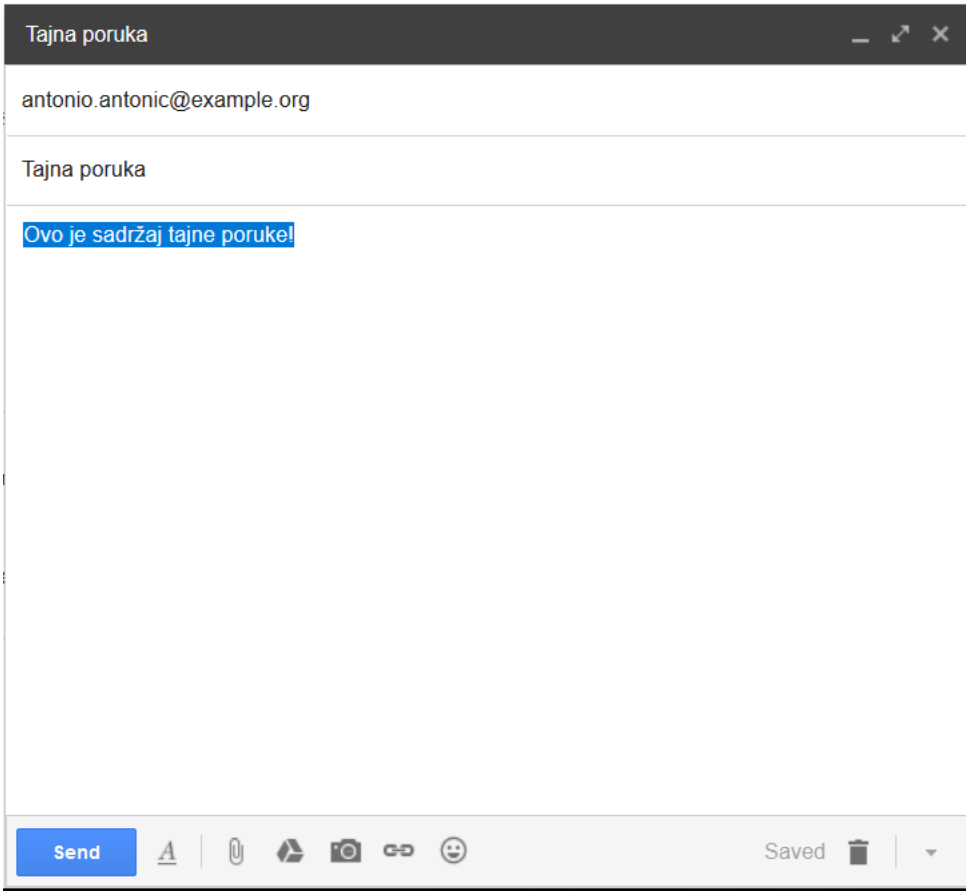


Potvrda ključeva sada je uspješno završena te pritiskom na ***Finish*** završavamo proces potvrde te možemo koristiti Antonijev certifikat.

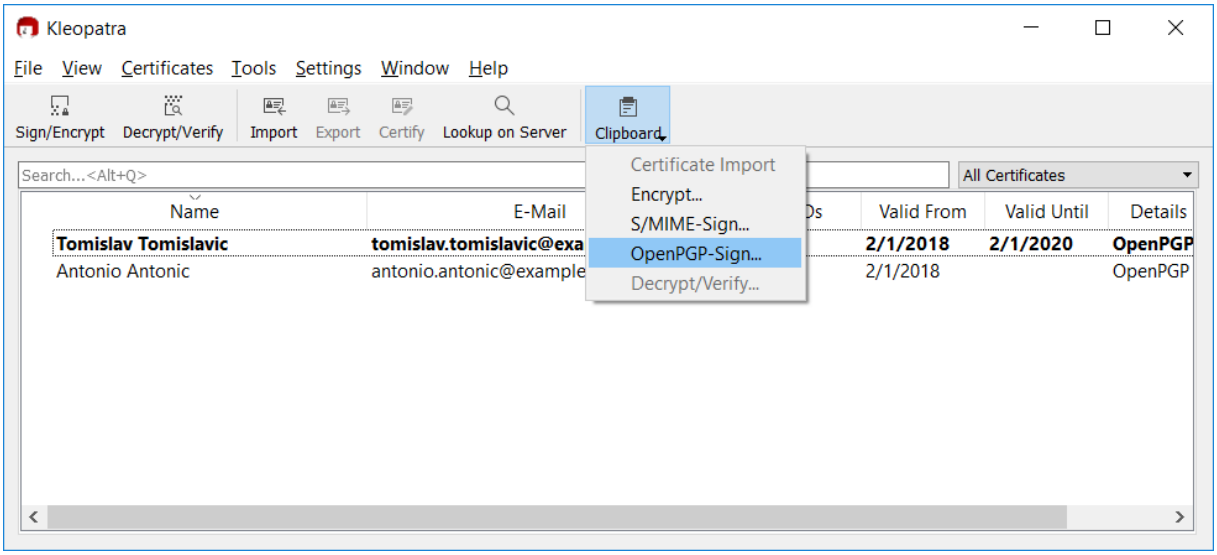


3.2.3 Šifriranje i potpisivanje poruke

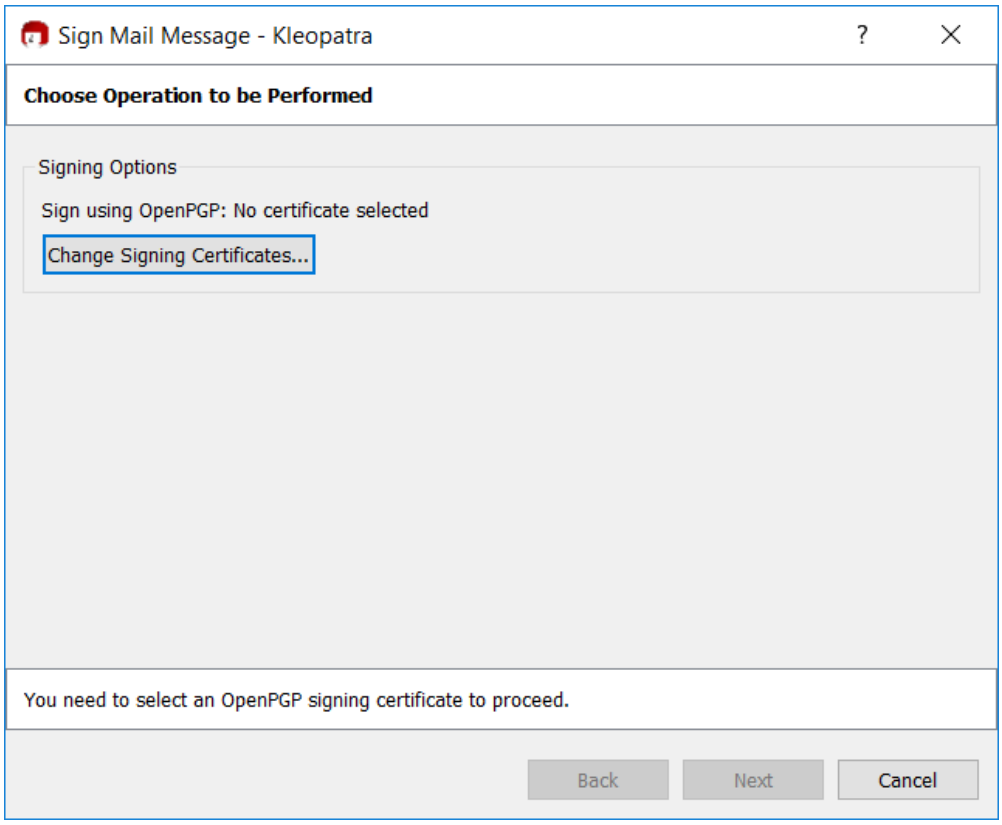
Ako Tomislav želi Antoniju poslati poruku e-pošte te osigurati njenu tajnost i vjerodostojnost, to može učiniti tako da poruku potpiše svojim privatnim ključem te ju šifrira Antonijevim javnim ključem. Sadržaj tajne poruke prvo je potrebno staviti u međuspremnik (eng. *clipboard*), npr. tako da označimo cijelu poruku te nakon desnog pritiska miša na nju odaberemo *Copy*.



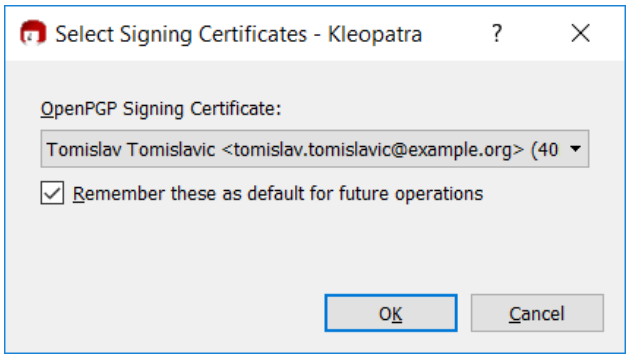
U alatu *Kleopatra* pritiskom na ikonu s natpisom ***Clipboard*** i odabirom ***OpenPGP-Sign…*** započinjemo proces digitalnog potpisivanja poruke.



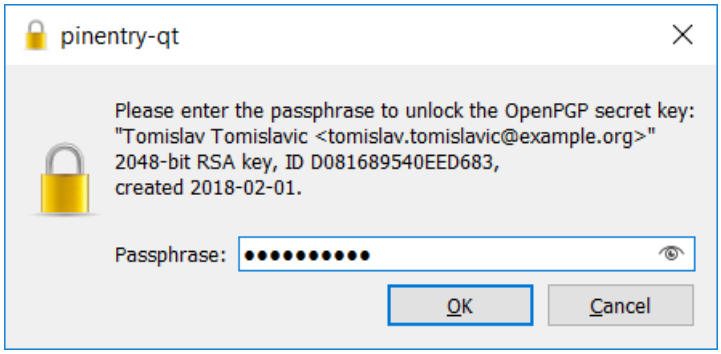
Sada je potrebno odabrati ključ kojim ćemo potpisati poruku. Taj proces započinjemo pritiskom na ***Change Signing Certificates...*** .



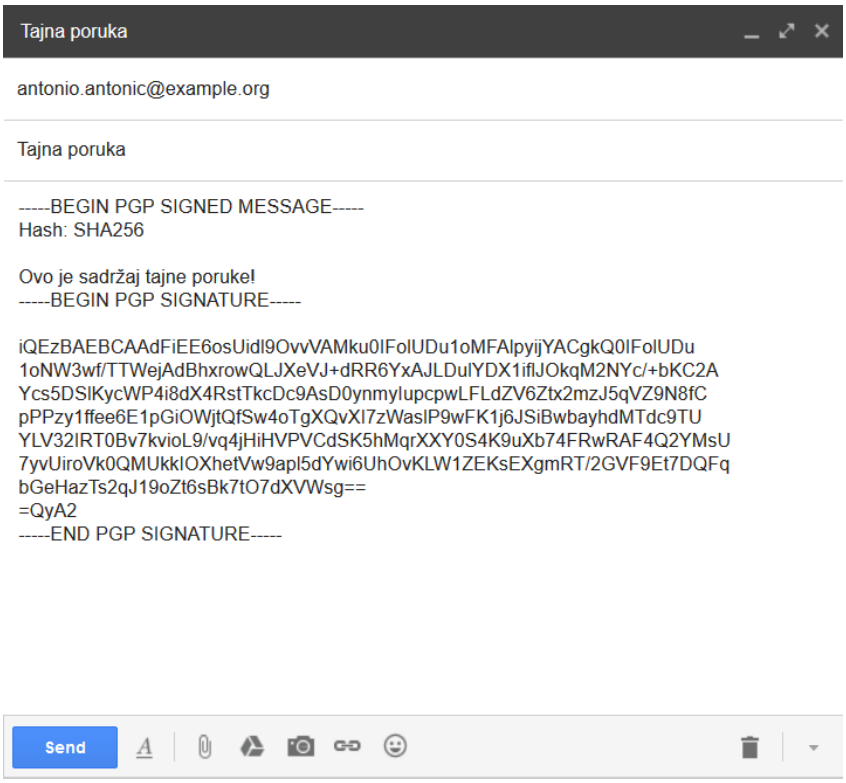
Potrebno je odabrati certifikat generiran na početku dokumenta.



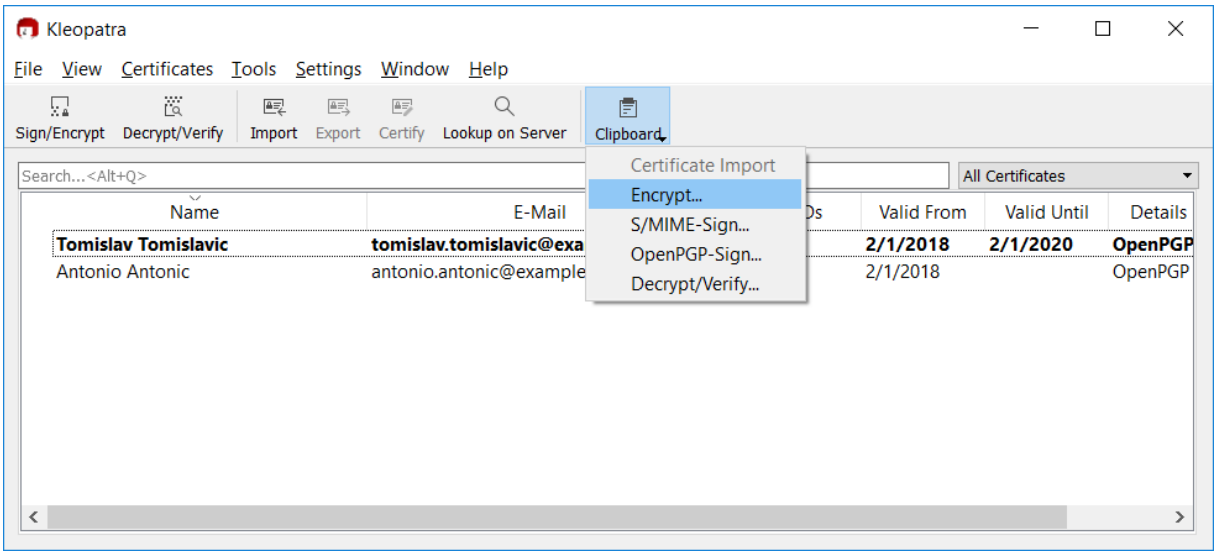
Zatim je potrebno upisati lozinku privatnog ključa koja je upisana u procesu generiranja ključeva kako bi poruku mogli potpisati s odabranim privatnim ključem.



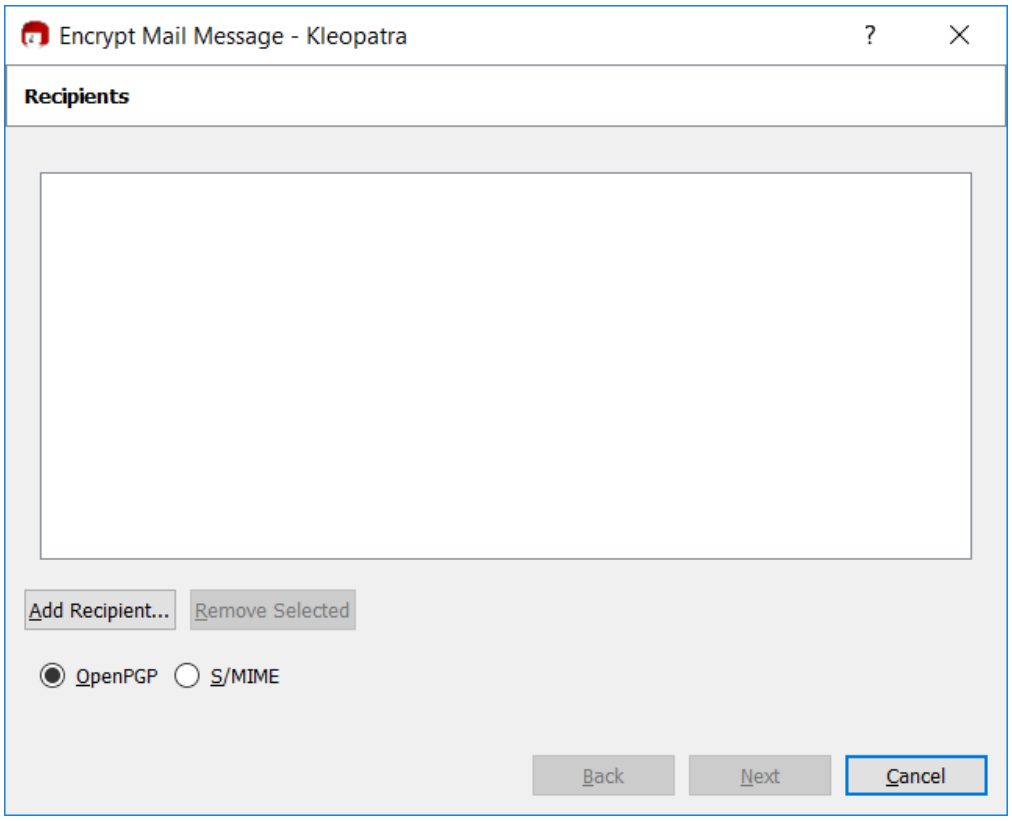
U međuspremniku se sada nalazi digitalno potpisana poruka. Za provjeru je možemo zalijepiti kao što je prikazano na donjoj slici:



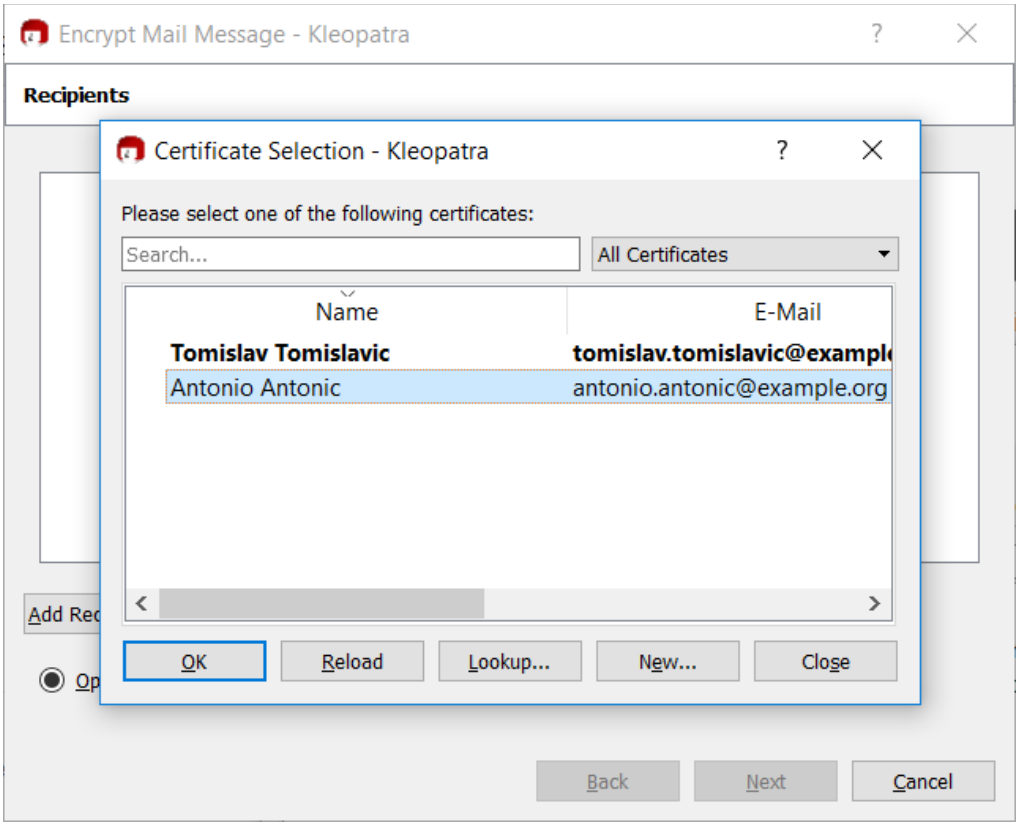
Kako bi poruka bila šifrirana, potrebno je opet pritisnuti na ikonu s natpisom *Clipboard*, no ovaj put odabrati „*Encrypt…*“.



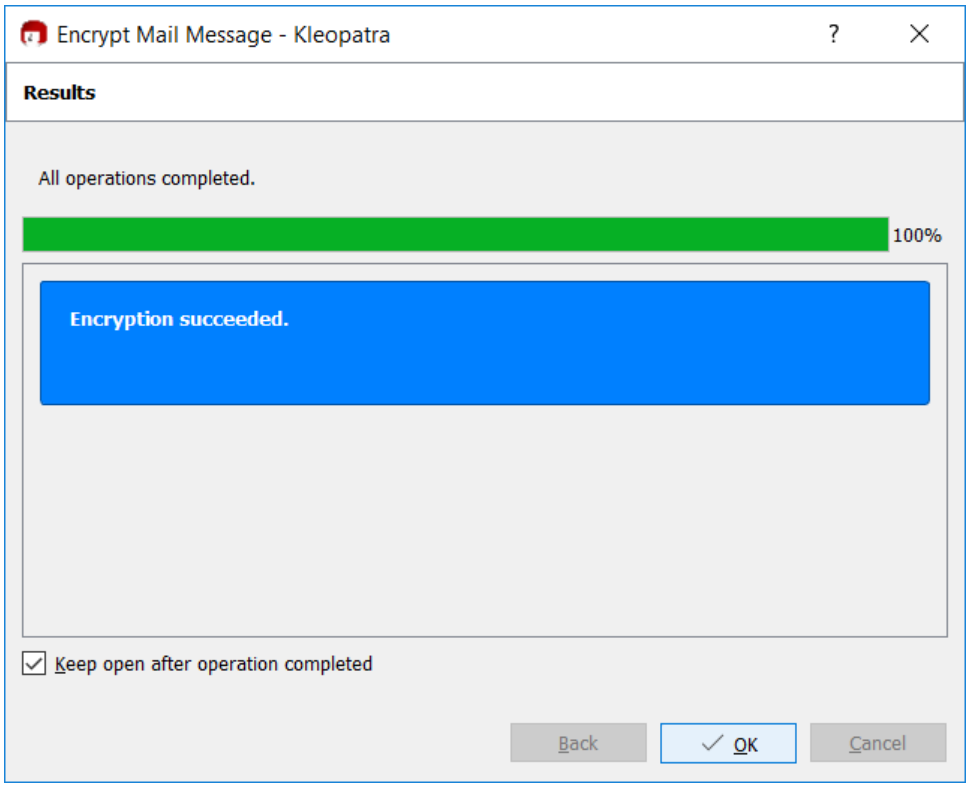
Pritiskom na ***Add Recipient...*** otvaramo prozor za dodavanje korisnika za kojeg šifriramo poruku.



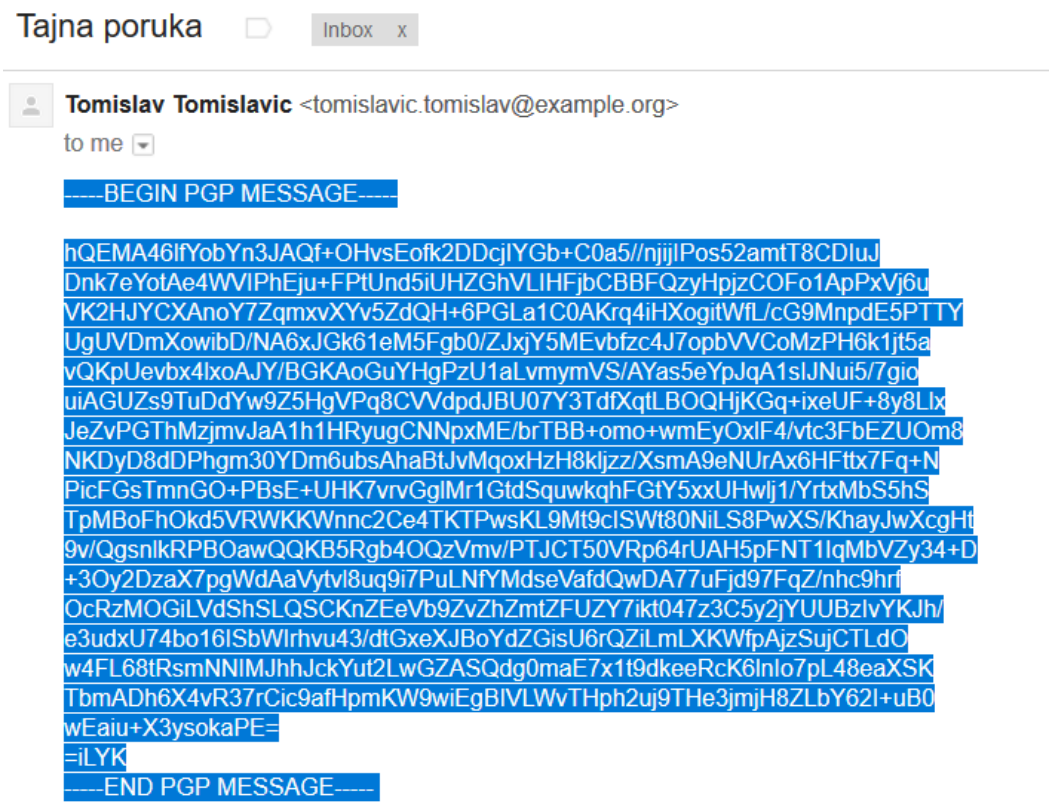
Potrebno je odabrati Antonijev ključ, pritisnuti na ***OK***, a zatim na ***Next***



Pritiskom na ***OK*** zatvara se prozor za šifriranje sadržaja međuspremnika, te se šifrirana poruka sada nalazi u međuspremniku.

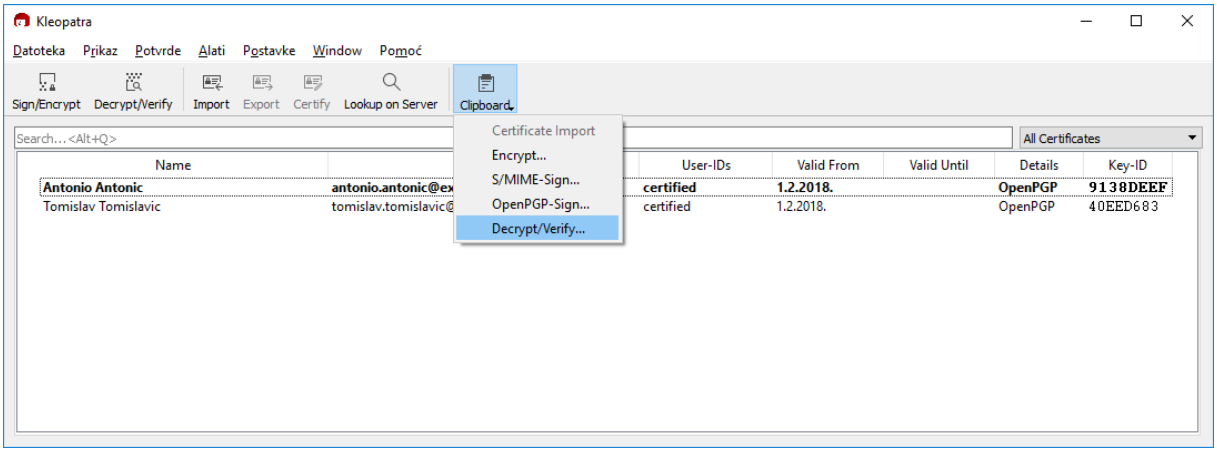


Takva šifrirana poruka se može iz međuspremnika zalijepiti u poruku e-pošte:

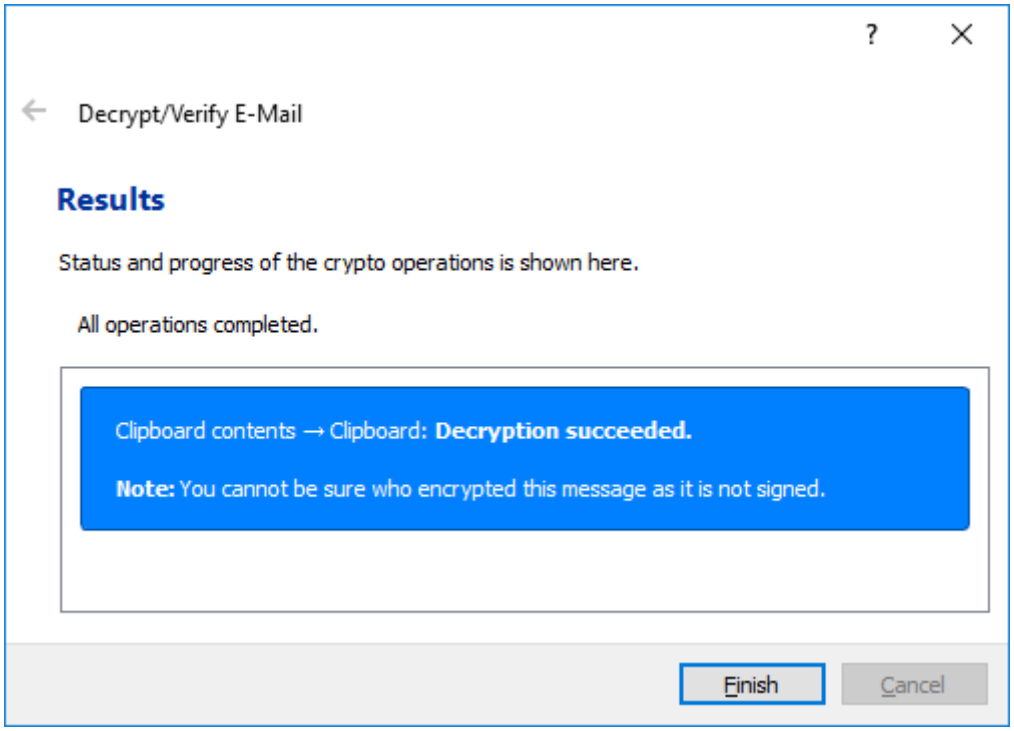


3.2.4 Dešifriranje i provjera potpisa

Nakon što je korisnik Antonio dobavio Tomislavov javni ključ i potvrdio da je to zbilja javni ključ koji pripada korisniku Tomislav, može dešifrirati i provjeriti ispravnost potpisa poruke. Označavanjem i kopiranjem poruke u međuspremnik taj proces može započeti. Otvaranjem alata Kleopatra te odabirom ikone ***Clipboard*** i odabirom ***Decrypt/Verify...*** počinje proces dešifriranja.

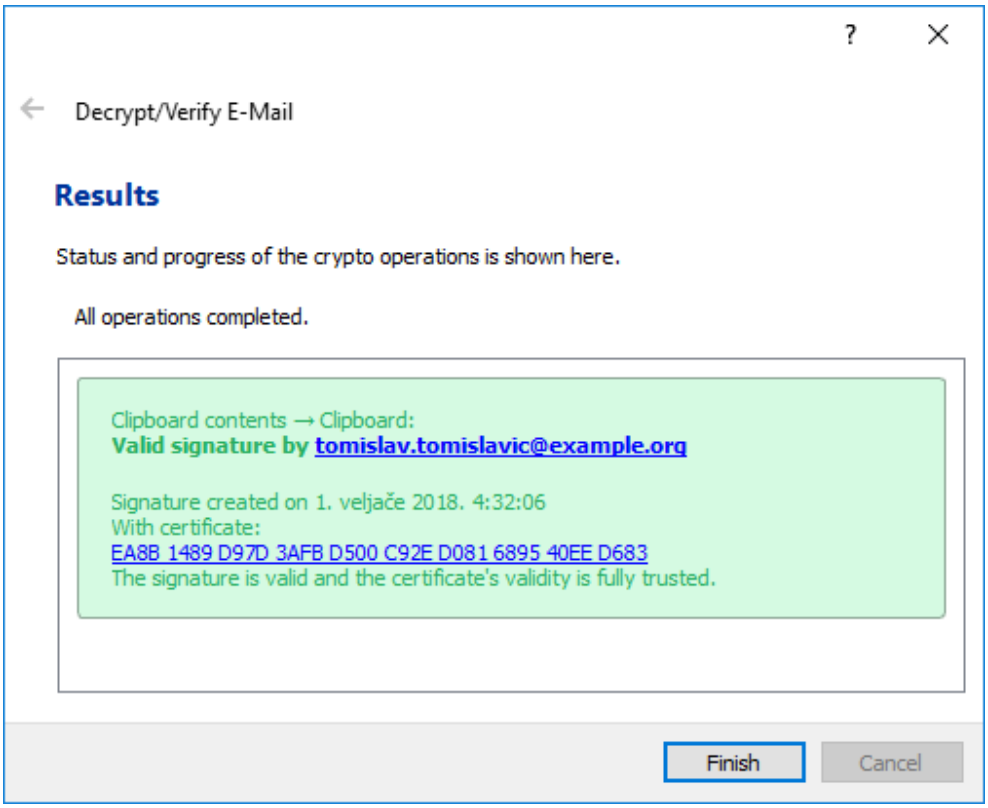


Šifrirana poruka iz međuspremnika je sada dešifrirana te takva spremljena u međuspremnik. Za zatvaranje prozora je potrebno pritisnuti ***Finish.***



Dešifriranu poruku u međuspremniku moguće je provjeriti tako da otvorimo uređivač teksta u koji možemo zalijepiti sadržaj poruke, kao što je prikazano u donjoj slici:

Ponavljanjem odabira ***Decrypt/Veryfy*** u alatu Kleopatra sada možemo provjeriti tko je digitalno potpisao poruku. Pokazuje se poruka da je poruka potpisana privatnim ključem koji odgovara javnom ključu korisnika Tomislav.



4 Zaključak

Ovaj dokument dao je kratki teoretski uvod u asimetričnu kriptografiju, javne i privatne ključeve te postupak šifriranja i digitalnog potpisivanja pomoću njih. Asimetričnom kriptografijom moguće je osigurati tajnost i vjerodostojnost poruka poslanim preko nesigurnih medija kao što je elektronička pošta.

Korištenjem ovih uputa moguća je praktična primjena asimetrične kriptografije alatom GnuPG na operacijskom sustavu Windows kroz programski paket Gpg4win. Korištenje alata opisano je na primjeru zaštite teksta elektroničke pošte, no GnuPG i Gpg4win je moguće primijeniti općenitije, primjerice i na zaštitu datoteka.

Postoje alati, primjerice dodaci za Web preglednike i dodaci za klijente e-pošte, koji djelomično automatiziraju proces prikazan u ovom dokumentu, no oni u suštini obavljaju isti postupak. Postupak opisan u ovom dokumentu dovoljan je za sigurno korištenje alata Gpg4win te je koristan i za općenito razumijevanje alata koji za zaštitu komunikacije koriste OpenPGP standard.