

Šifrovanje elektronske pošte za MacOSX

CRYPTOPARTY SERBIA

July 23, 2016

Contents

1	Kratak uvod	2
2	Instalacija GpgTools programa	3
2.1	Generisanje GPG ključeva	7
3	Šifrovanje poruke primaocu pošte	10
4	Šta vidi mejl provajder	14
5	Dešifrovanje primljene šifrovane poruke	15

1 Kratak uvod

Ovo uputstvo će vam pokazati kako da šifrujete elektronsku poštu na operativnom sistemu Mekintoš koristeći podrazumevanog klijenta elektronske pošte tj. imejl klijenta na Mekintošu.

Mekinoš operativni sistem nije u potpunosti otvorenog koda, kao ni softver koji dolazi uz operativni sistem, pa ne treba imati previše poverenja u privatnost ličnih podataka na ovom operativnom sistemu. Kada je to rečeno pređimo na uputstvo za konfigurisanje **GPG** programa za Mac.

2 Instalacija GpgTools programa

Najpre je potrebno da preuzmete program **GpgTools** sa gpgtools.org. To je program zadužen za kreiranje **GPG** ključeva potrebnih za šifrovanje dešifrovanje poruka, digitalno potpisivanje i provere digitalnih potpisa poruka.

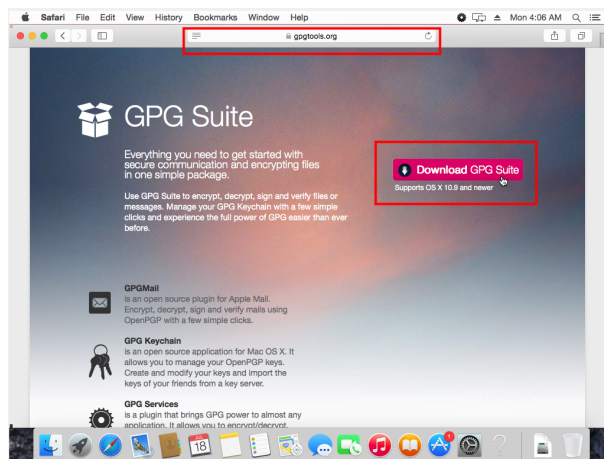


Figure 1: Preuzmite GpgTools sa interneta

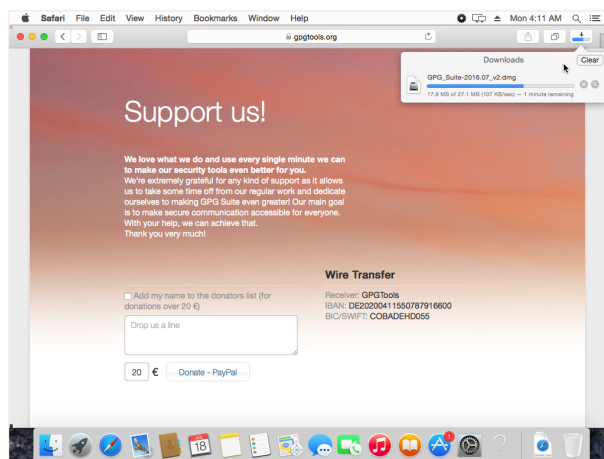


Figure 2: Kada se završi preuzimanje **Gpgtools** programa, pokrenite ga.



Figure 3: Po pokretanju **Gpgtools** programa idaberite **Install** opciju da biste instalirali program

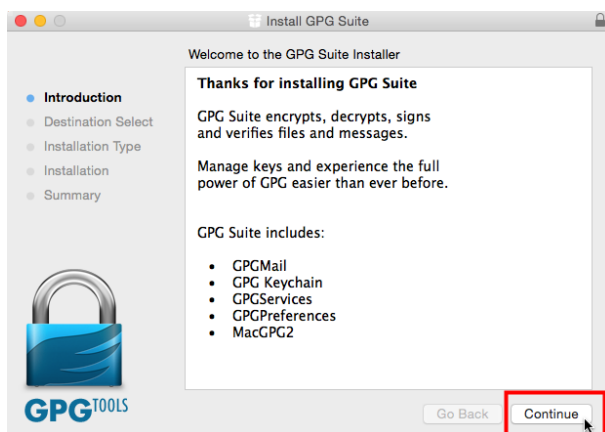


Figure 4: Prođite kroz jednostavan proces instalacije..

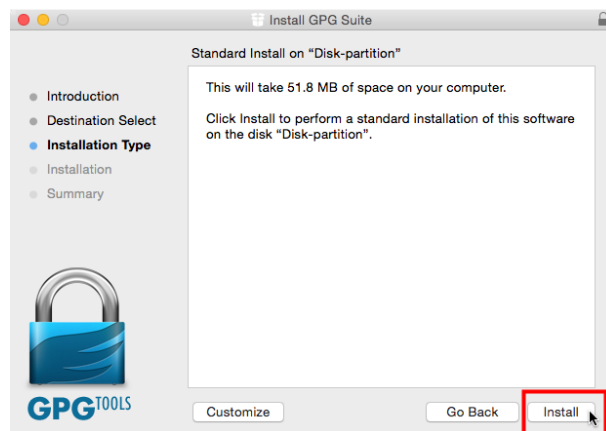


Figure 5: standardna instalacija će uraditi sve potrebno za vas automatski.

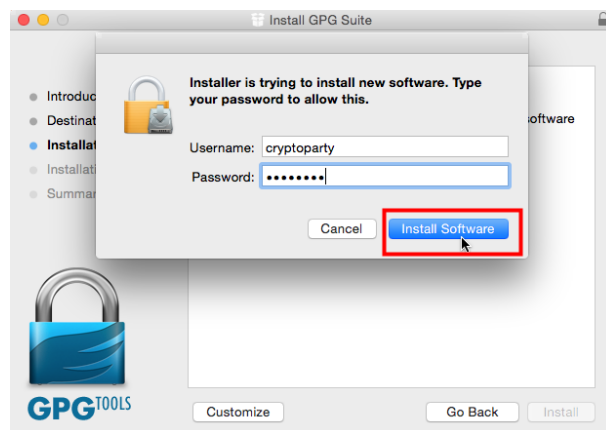


Figure 6: Naravno, tražiće vam šifru korisnika sistema kako bi se program instalirao.

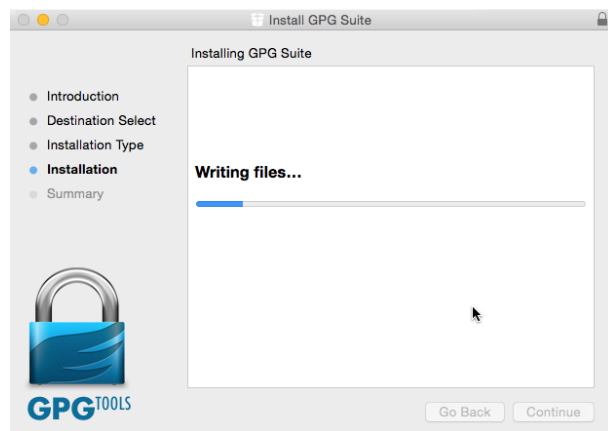
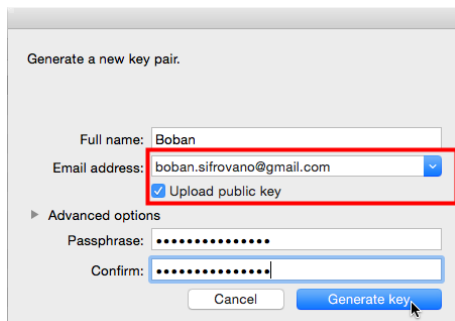


Figure 7: I kada završi sa upisom podataka proces instalacije je gotov.

2.1 Generisanje GPG ključeva



Generate a new key pair.

Full name: Boban

Email address: boban.sifrovano@gmail.com

☒ Upload public key

► Advanced options

Passphrase:

Confirm:

Cancel Generate key

Figure 8: Sada unesite email adresu za koju generišete ključeve i podesite šifru za te ključeve

Ovu šifru morate zapamtiti ili zapisati negde, jer će vam trebati da bi ste dešifrovali primljene šifrovane poruke.

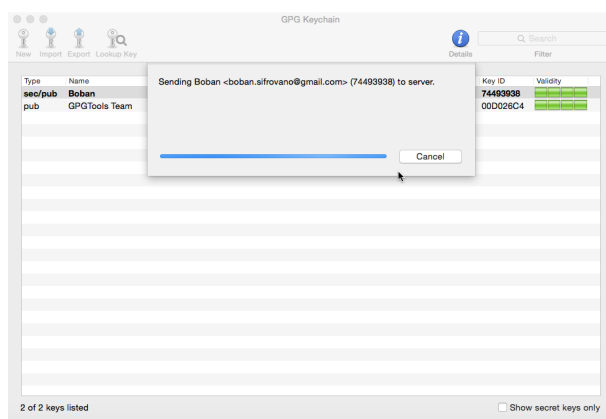


Figure 9: Kada i to završite, **Gpgtools** će vaš novi javni ključ poslati na server javnih ključeva kako bi drugi ljudi koristili taj javni ključ da vam pošalju šifrovane poruke.

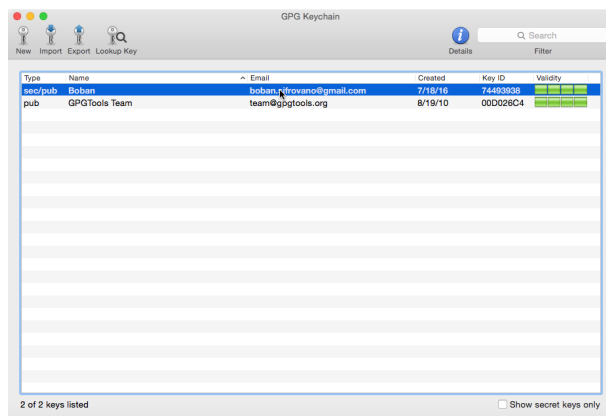


Figure 10: Vaš novi ključ će biti prikazan u **GpgTools** bazi ključeva.



Figure 11: Sada je potrebno da podesimo i mejl klijenta za isti mejl nalog za koji smo kreirali ključeva, ukoliko to već nismo ranije uradili.

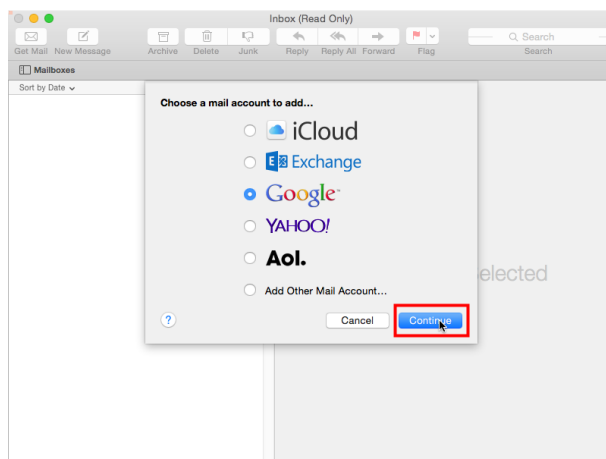


Figure 12: Konkretno mi koristimo Gmail u ovom uputstvu, a vi podesite za vašeg mejl provajdera.

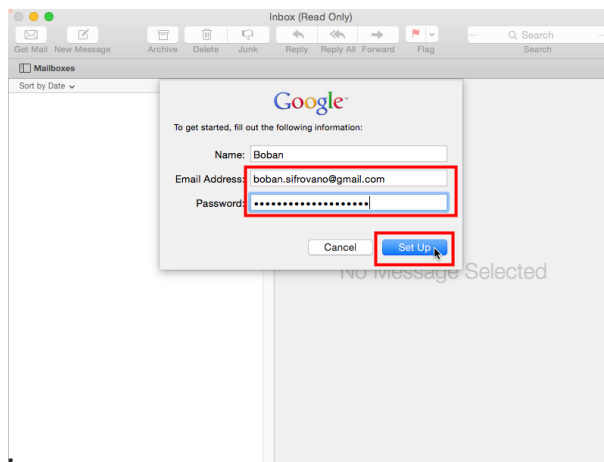


Figure 13: Pdesite istu mejl adresu kao onu za koju ste kreirali ključeve.

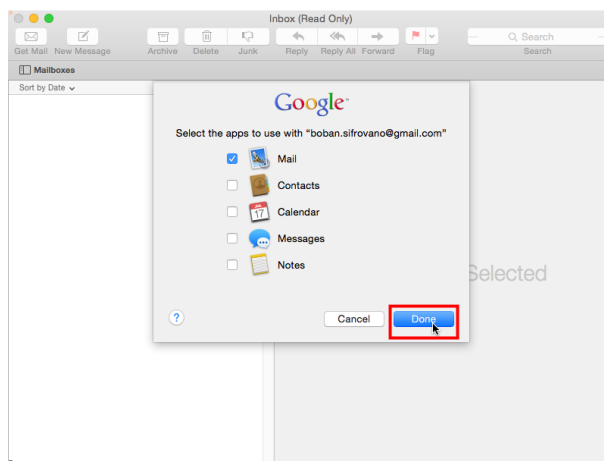


Figure 14: Koristimo mejl naravno.

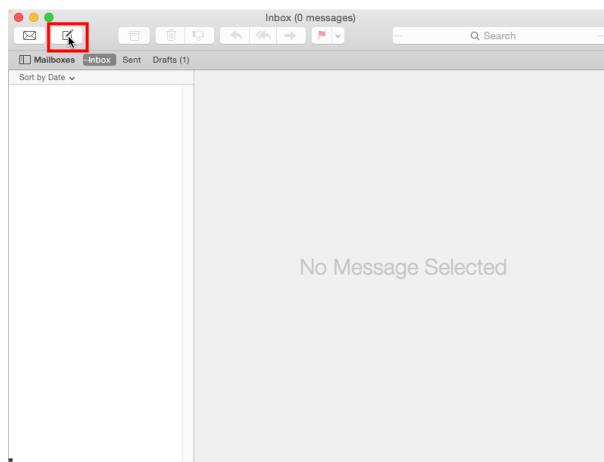


Figure 15: Sada će mo pokušati da napišemo šifrovanu poruku.

3 Šifrovanje poruke primaocu pošte

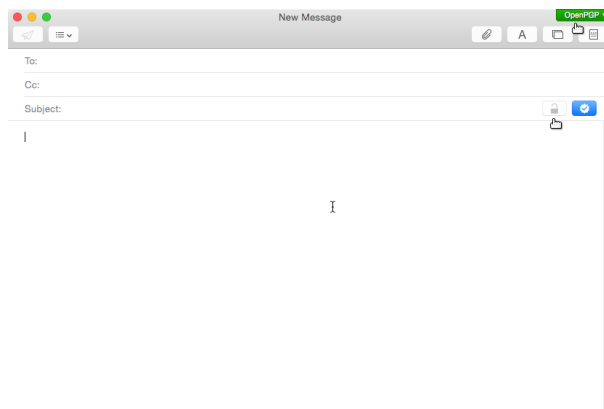


Figure 16: Primetite kako u gornjem desnom uglu prozora za sastavljanje poruke ima zeleni pravouganik sa zankom **OpenPGP**. To znači da je **Gpgtools** integrisan u mejl kljijenta. Takođe primetite da je sivi katanac otključan. Da bi šifrovali poruku za nekog primaoca, prvo moramo imati njegov javni ključ (ako primaoc koristi GPG tj. ima svoje ključeve)



Figure 17: Pa ponovo otvaramo **Gpgtolls** kako bi smo iz njega tražili javni ključ osobe kojoj šifrujemo mejl.

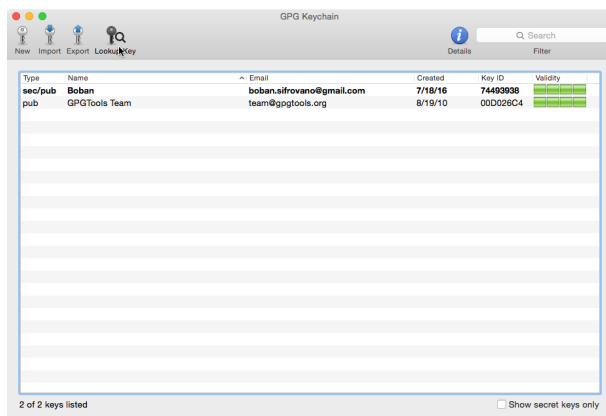


Figure 18: Tražimo ključeve.

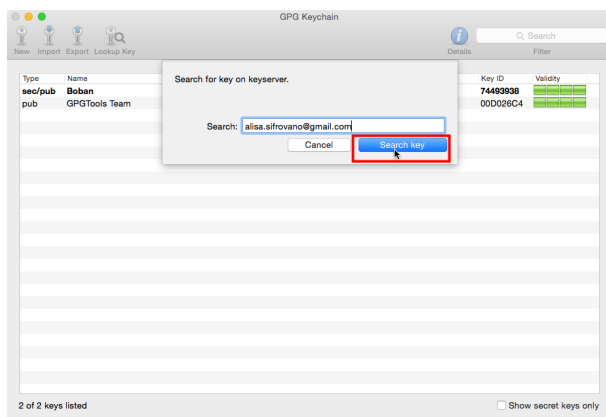


Figure 19: Unosimo mejl adresu onoga čiji nam javni ključ treba, tj onome kome pišemo.

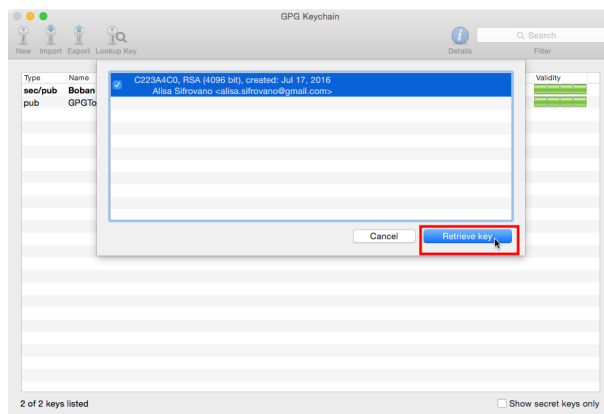


Figure 20: ako ključ postoji, biva pronađen i mi ga preuzimamo.

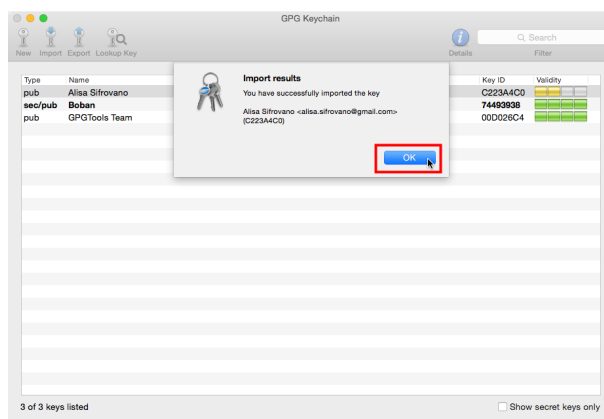


Figure 21: Poruka o uspešnom pribavljanju javnog novog javnog ključa.

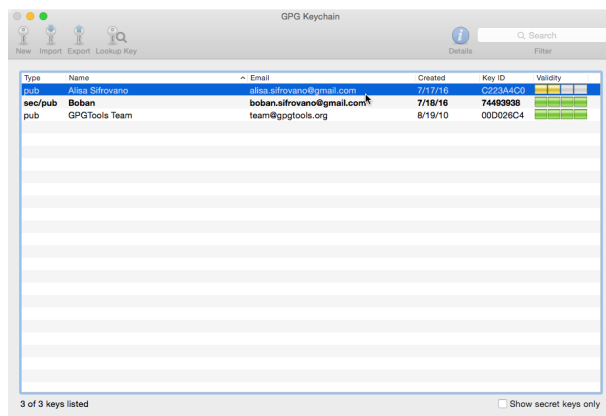


Figure 22: Videće te novi ključ u **Gpgtools** programu.

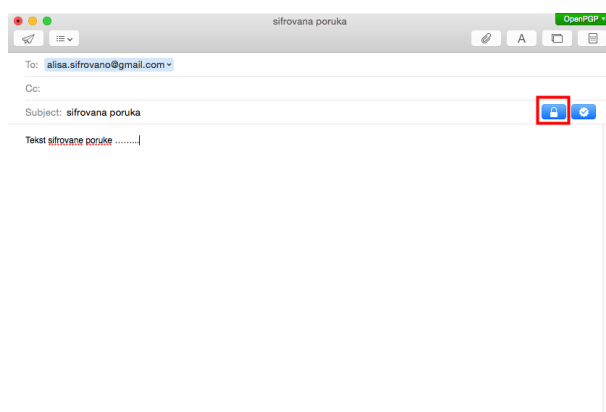


Figure 23: I sada kada se vratimo na sastavljanje našeg šifrovanog mejla, posle unosa adrese primaoca poruke, videće te da se katanac promenio u plavu boju i da sada poruka mož da se šifrjuje.

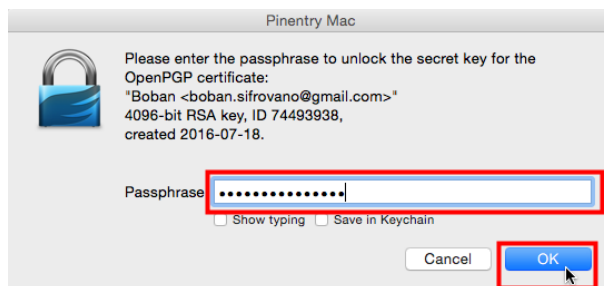


Figure 24: Kada završite pisanje poruke i kliknete na dugme za slanje (ikonica papirnog aviončića), tražiće vam šifru za **GPG**, kako bi otključao vaš tajni ključ i njime digitalno potpisao poruku koju šaljete.

4 Šta vidi mejl provajder

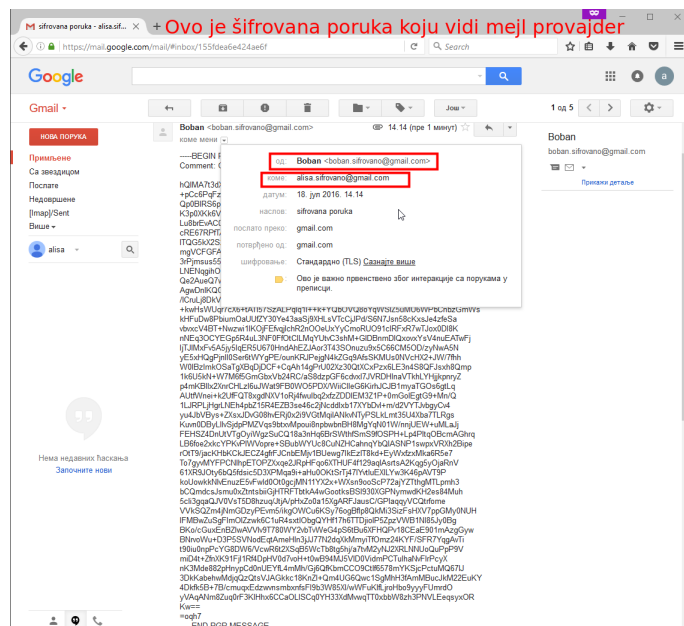


Figure 25: Vaš mejl provajder, kao i mejl provajder osobe kojoj ste poslali šifrovanu poruku mogu videti samo naslov poruke i ko kome šalje šifrovanu poruku, ali ne i sadržaj iste.

5 Dešifrovanje primljene šifrovane poruke

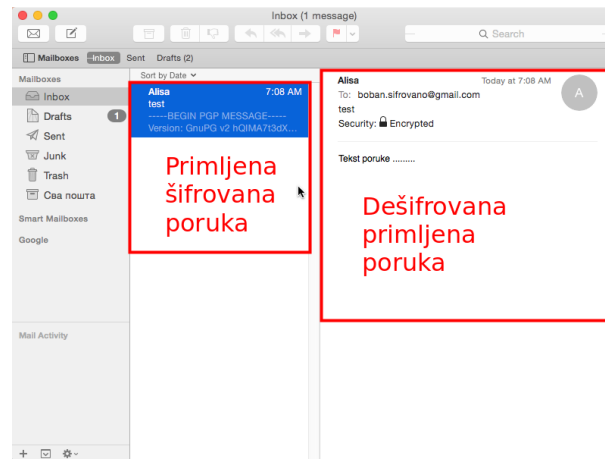


Figure 26: Kada primite novu poruku u mejl klijentu, ako je ona šifrovana klijent će to prepoznati i ponuditi da dešifruje automatski ako unesete šifru za vaš tajni **GPG** ključ.