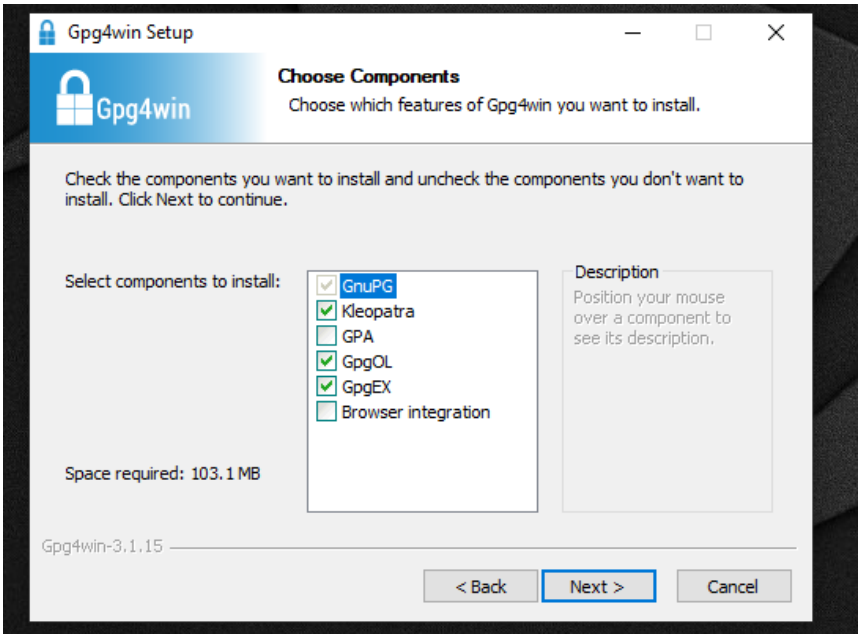
Inštalácia PGP – Outlook

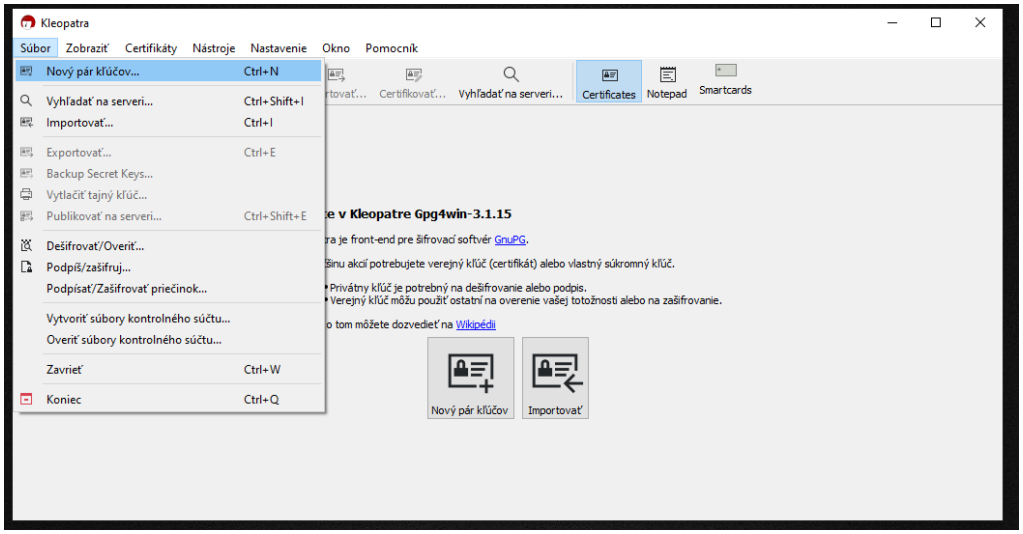
1. Stiahnite si najnovšiu verziu softvéru gpg4win - https://www.gpg4win.org/

2. Spustíme .exe

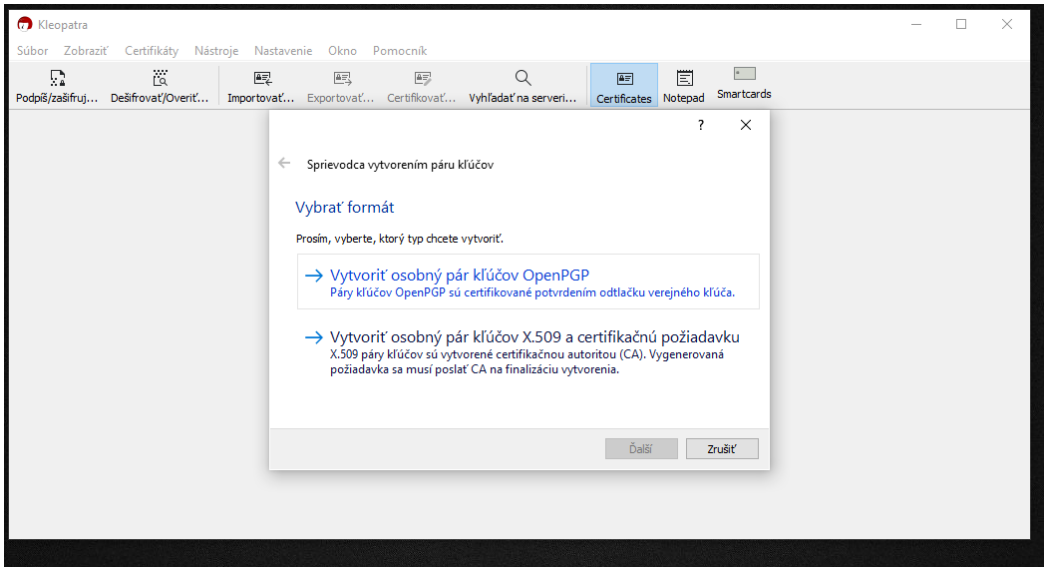
3. Nechávame zaškrtnuté všetko v základnom stave. Pre nás je najdôležitejšie mať zaškrtnuté políčka GnuPG (balík) a softvér Kleopatra spolu s doplnkom GpgOL.



4. Ak ste doteraz nepoužívali šifrovanie pomocou PGP kľúčov, vytvorte si pomocou softvéru Kleopatra svoj PGP pár. Softvér Kleopatra slúži aj ako naša databáza kľúčov.



5. Vytvárame osobný PGP pár – je zložený z Verejného a Súkromného kľúča

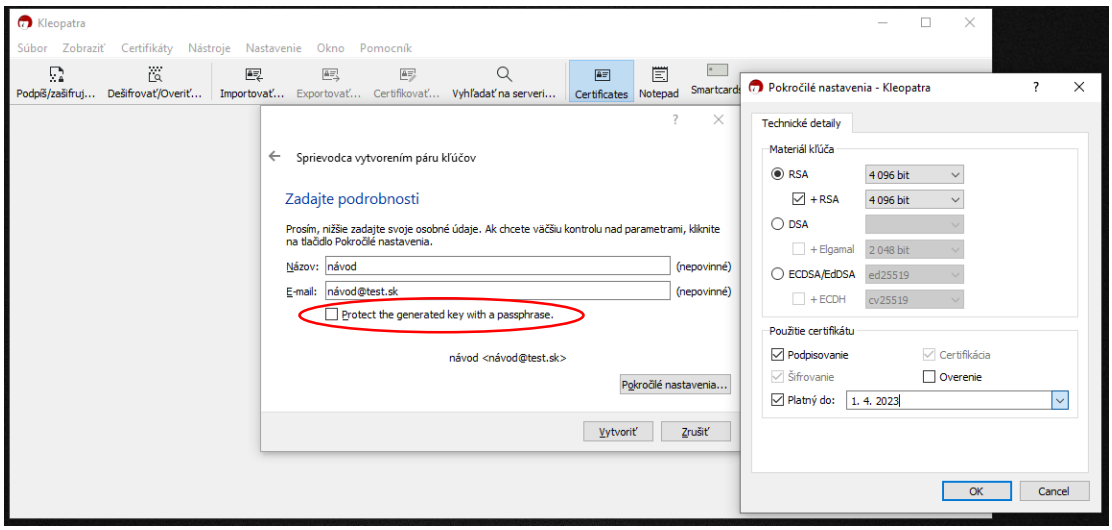


6. Vyplníme názov (Vaše meno) a E-mail = identita kľúčového páru (email, z ktorého budete posielať šifrované emaily, identity sa dajú aj pridávať pre viacej emailov).

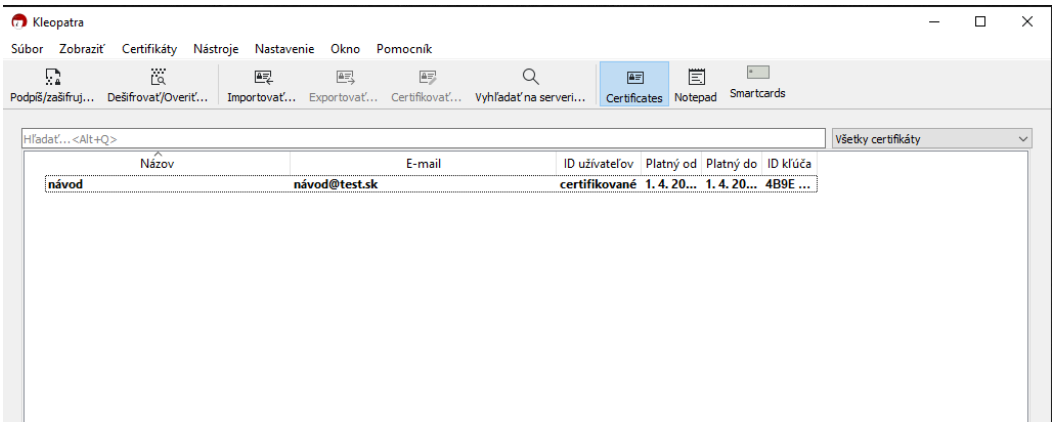
• Zaškrtneme aj možnosť chrániť svoj kľúčový pár heslom ! Heslo dobre uschovávame, bude ho od nás emailový klient pýtať pri šifrovaní, alebo dešifrovaní správy.

• V rozšírených nastaveniach si môžete vybrať veľkosť šifrovacieho kľúča typu RSA – odporúčaná veľkosť je 3072 (predvolené nastavenie) alebo 4096 bitov.

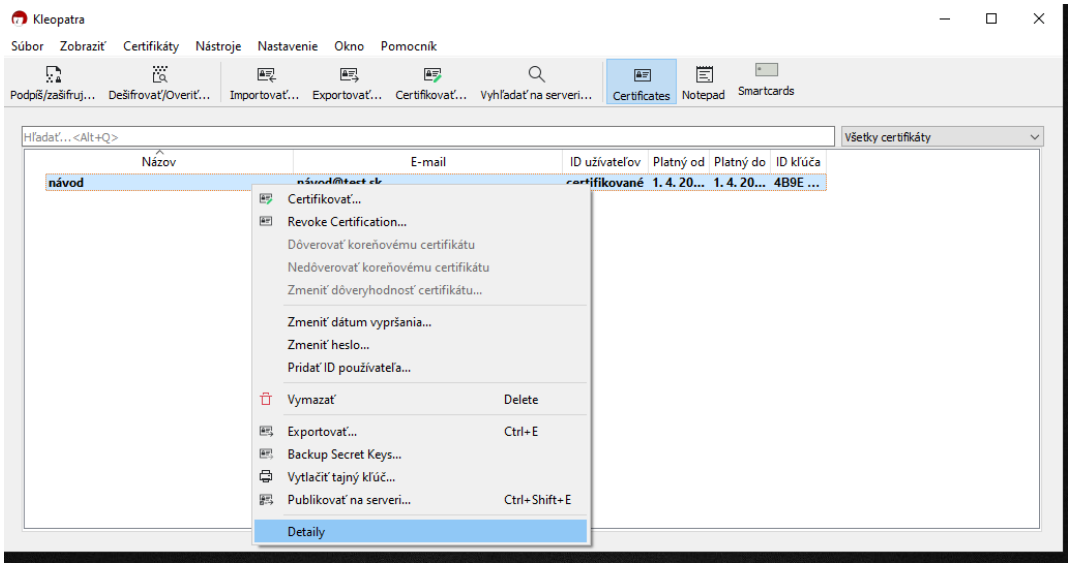
• Rovnako v pokročilých nastaveniach vyberáme aj platnosť kľúčového páru. Základná platnosť sa nastavuje na 2 roky. Po 2 rokoch sa kľúčový pár revokuje (vyhlási sa za neplatný). Následne sa vytvára nový (takéto zaobchádzanie je potrebné z dôvodu bezpečnosti).

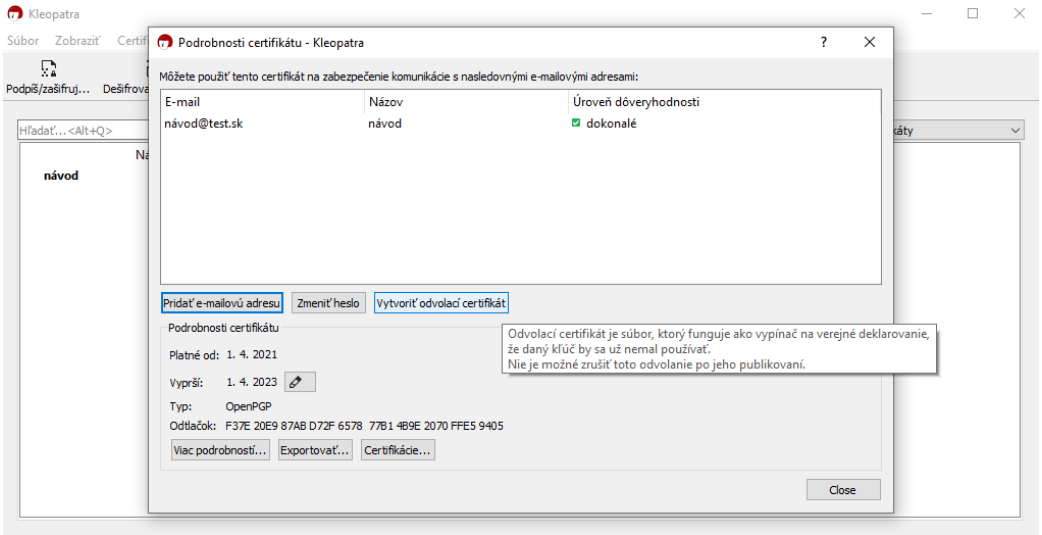


7. Po vytvorení kľúčového páru, budeme vidieť svoj kľúčový pár zvýraznený hrubým písmom. Hrubé písmo záznamu kľúča značí, že sa v zázname nachádza verejný aj súkromný PGP kľúč. To je dôležité, keď máme v zozname väčšie množstvo verejných kľúčov budúcich adresátov šifrovaných emailov, aby sme v prípade potreby rýchlejšie našli svoj PGP pár.

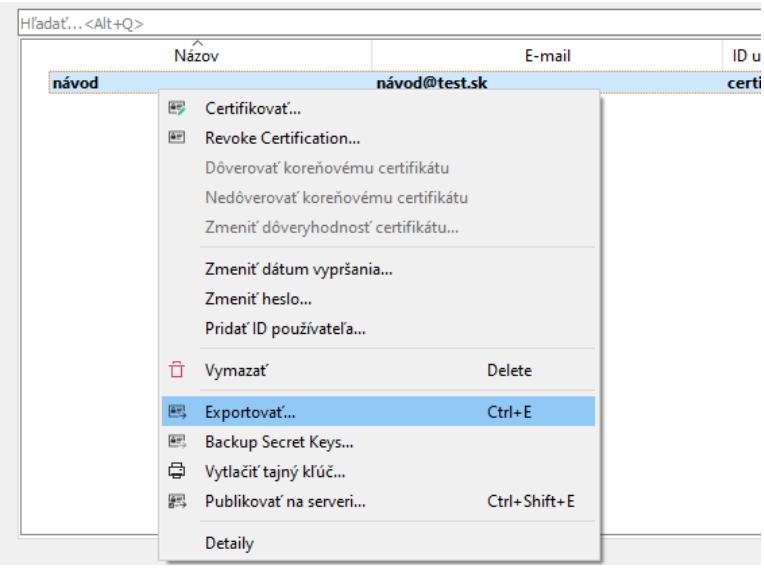


8. V záujme zachovania bezpečnosti si vytvoríme revokačný certifikát, ktorý si bezpečne uložíme. Revokačný certifikát sa používa v prípade, ak nám je odcudzený (alebo kompromitovaný) súkromný kľúč, prípadne keď vyprší platnosť kľúčového páru.

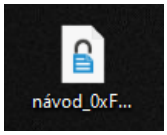




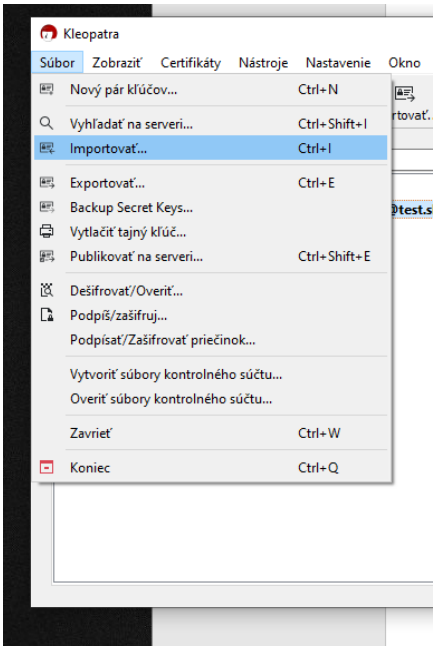
9. Klikneme pravým tlačidlom myši a vyberieme exportovať. Exportuje sa nám verejný kľúč, ktorý rozpošleme kontaktom s ktorými chceme šifrovane komunikovať. Každý s kým chceme šifrovane komunikovať nám musí rovnako poslať svoj verejný kľúč.

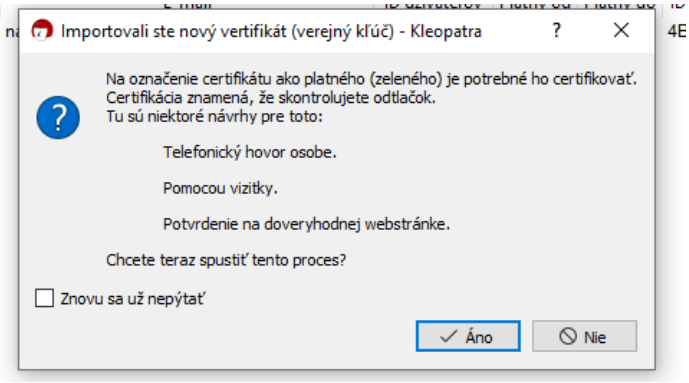


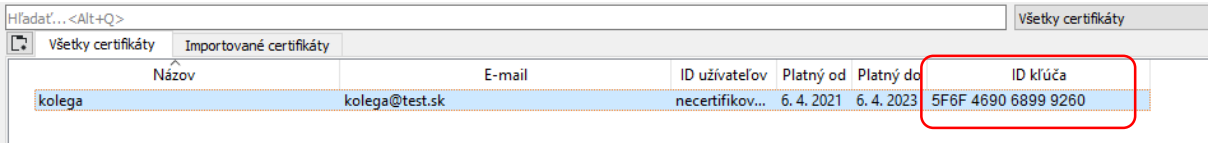
10. Verejný kľúč sa uloží s názvom „názov_odtlačok_verejného_kľuča“. Odtlačok verejného kľúča predstavuje jednoducho overiteľný identifikátor.



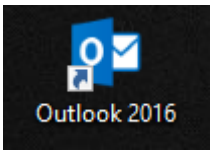
11. Potom ako nám adresát (napríklad kolega) pošle svoj verejný kľúč, importujeme ho cez súbor/importovať. Po importovaní verejného kľúča je odporúčané overiť si ID kľúča (odtlačok) prostredníctvom iného kanálu, napr. telefonicky, cez Signal alebo osobne. ID kľúča je verejná informácia, bežne sa umiestňuje napr. do textového podpisu v emaily. Po overení ID kľúča môžeme začať posielať šifrované emaily.



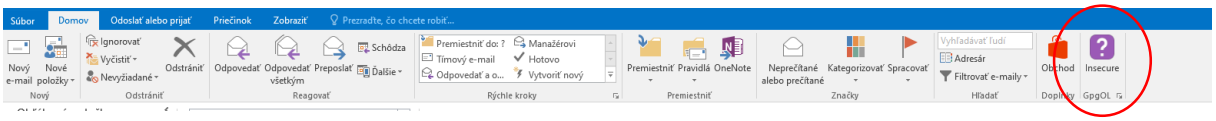




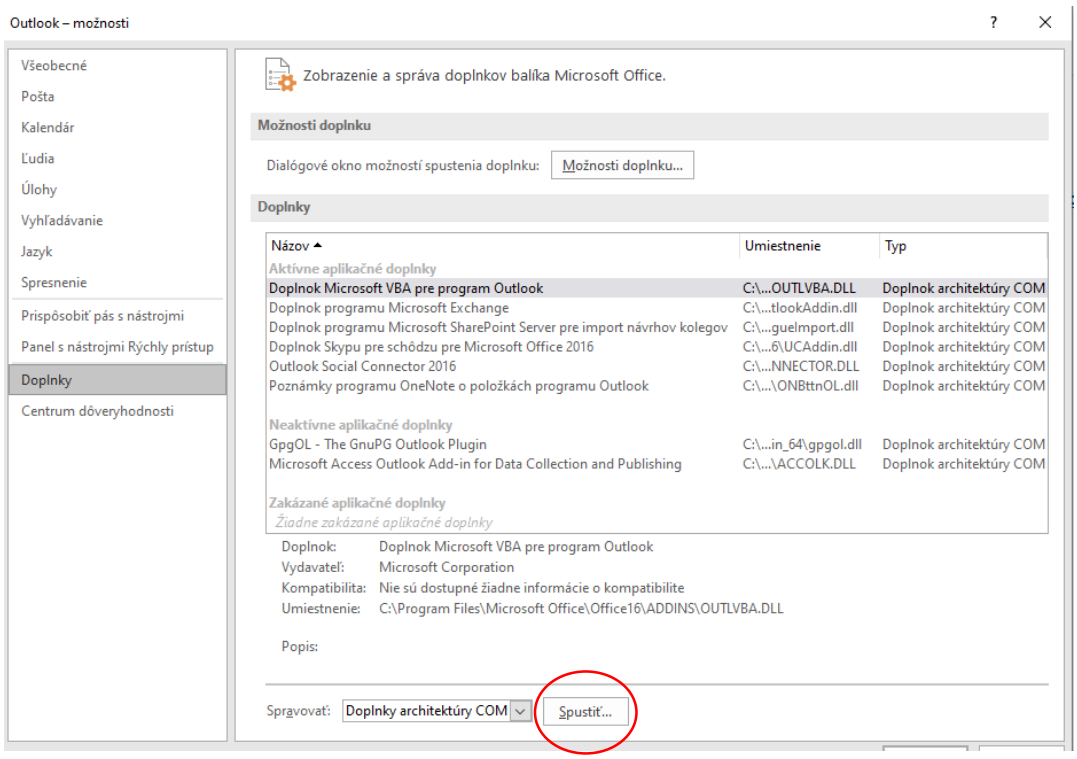
12. Otvoríme si mailového klienta v tomto prípade Outlook.



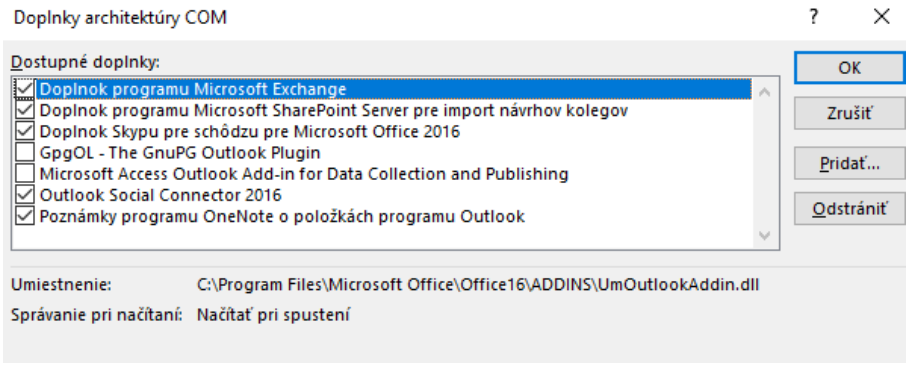
13. Ak úkon prebehol správne, na lište s nástrojmi by sa nám mal na pravom konci objaviť fialový otáznik.



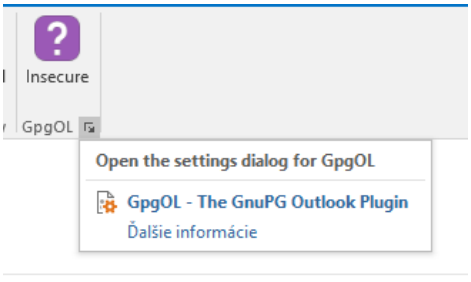
14. Ak došlo k chybe, treba ísť do Súbor/Nastavenia/Doplnky, kliknúť dole na „Spustiť“.



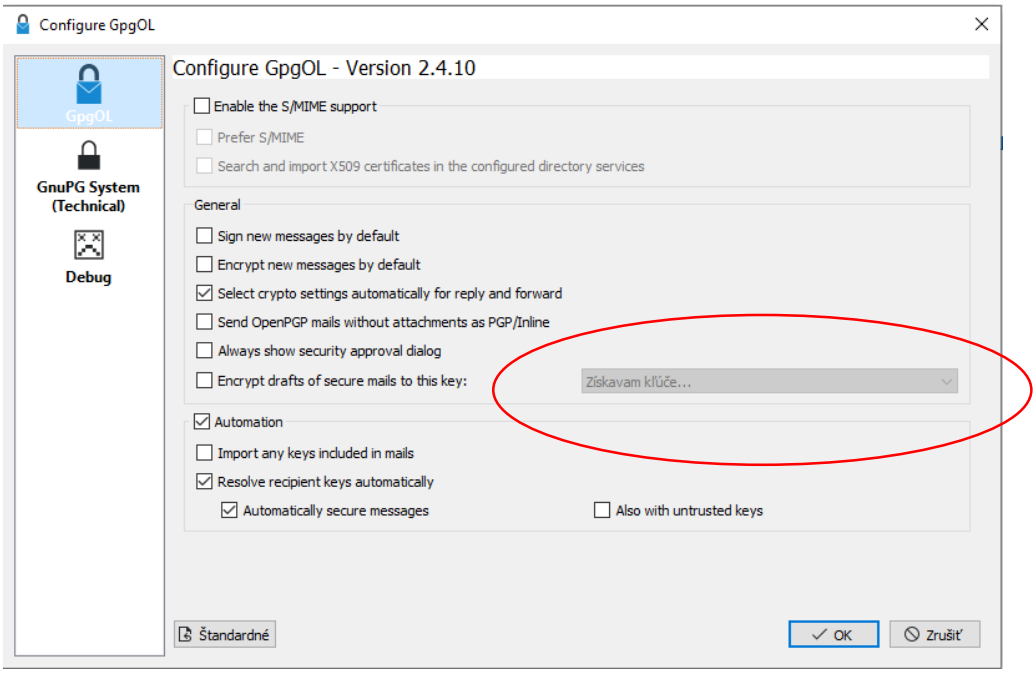
Odznačiť GpgOL, potvrdiť „OK“, reštartovať Outlook. Opäť sa vrátiť do tohto menu a vybrať - označiť GpgOL, potom potvrdiť „OK“.



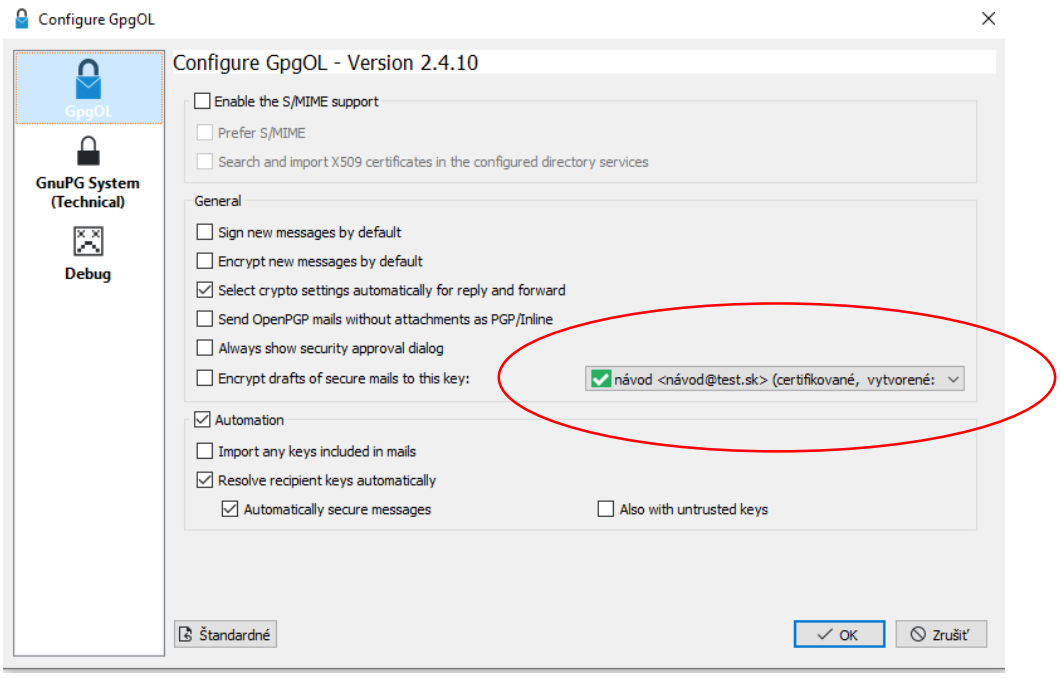
15. Ak sa nám zobrazí fialový otáznik, pozrieme si, či je všetko správne a či nám Kleopatra komunikuje s doplnkom.
Rozklikneme v pravom spodnom rohu ikonu a dostaneme sa do nastavení.



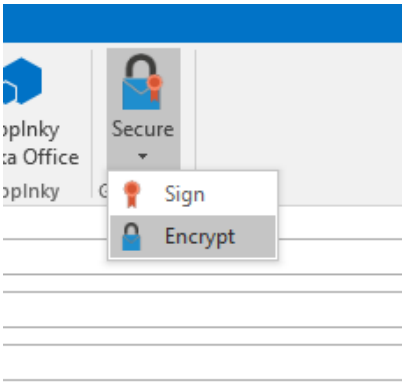
16. V nastaveniach doplnku nás zaujíma, či si doplnok stiahol náš PGP kľúčový pár.



Chvíľu to môže trvať, nakoniec by sa nám mal objaviť. Pokračujeme stlačením tačidla „OK“.



17. V tomto momente sme schopní posielať šifrované a kryptograficky podpísané emailové správy. V okne nová správa alebo pri odpovedi na správu klikneme na modrý zámok na pravej strane poľa nástrojov a vyberieme „podpísať“ a „šifrovať“, čím zaručíme dôvernosť a integritu obsahu správy. Je vhodné zvoliť obidve funkcie, aby sme zaručili, že správu počas prenosu nemôže nikto prečítať (šifrovanie) a taktiež pozmeniť (podpísanie).



18. Na záver ešte niekoľko odporúčaní :

• Za žiadnych okolností nikdy neposielajte nikomu svoj súkromný kľúč.

• Po výmene verejných kľúčov s adresátmi je vhodné overiť si ID kľúčov/odtlačky.

• Je vhodné si nastaviť heslo ku svojmu kľúčovému páru, ak ste tak neurobili pri jeho vytvorení (klik pravým tlačidlom na svoj kľúčový pár v Kleopatre, detaily – zmeniť heslo). Heslo je vhodné dobre uschovať v password manageri (napríklad Keepass, Bitwarden).

• Revokačný certifikát je potrebné dobre uložiť, bude potrebný pri revokovaní (zneplatnení) kľúčového páru po uplynutí platnosti alebo v prípade odcudzenia súkromného kľúča.

• Po uplynutí platnosti a revokovaní nášho PGP páru si súkromný kľúč stále uchovávame, aby sme nestratili možnosť dešifrovať svoje staršie správy.