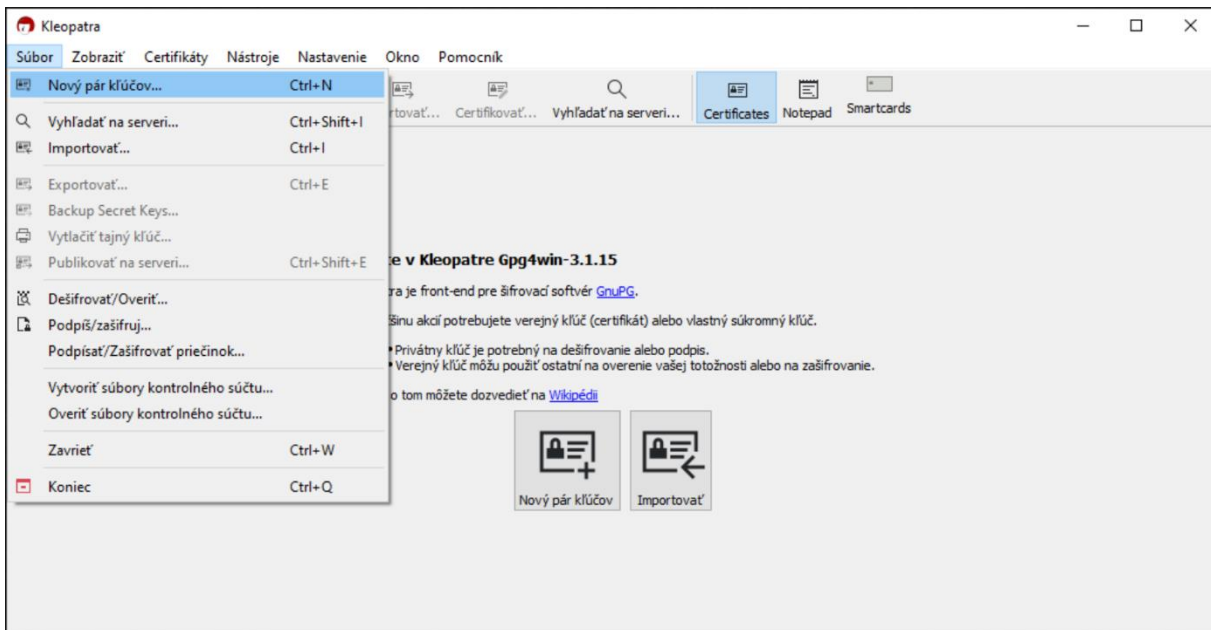
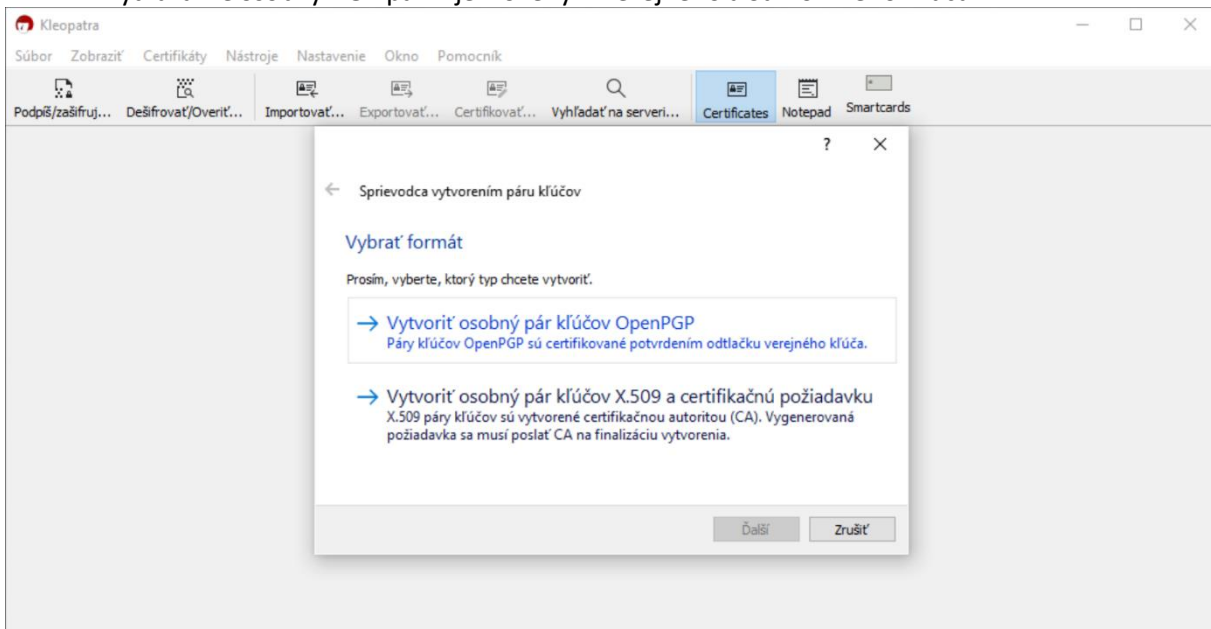


Vytvorenie páru PGP klúčov

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

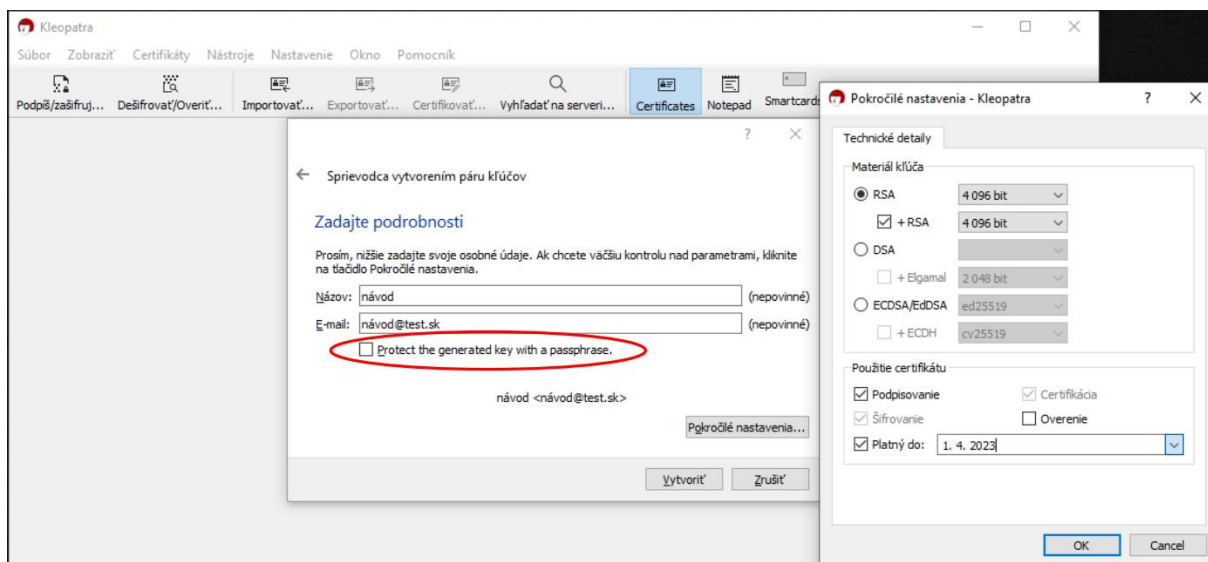


2. Vytvárame osobný PGP pár – je zložený z Verejného a Súkromného klúča



3. Vyplníme názov (Vaše meno) a E-mail = identita klúčového páru (email, z ktorého budete posilať šifrované emaily, identity sa dajú aj pridávať pre viacej emailov).
 - a. Zaškrtneme aj možnosť chrániť svoj klúčový pár heslom ! Heslo dobre uschováme, bude ho od nás emailový klient pýtať pri šifrovaní, alebo dešifrovaní správy.
 - b. V rozšírených nastaveniach si môžete vybrať veľkosť šifrovacieho klúča typu RSA – odporúčaná veľkosť je 3072 (predvolené nastavenie) alebo 4096 bitov.
 - c. Rovnako v pokročilých nastaveniach vyberáme aj platnosť klúčového páru. Základná platnosť sa nastavuje na 2 roky. Po 2 rokoch sa klúčový pár revokuje (vyhlási sa za

neplatný). Následne sa vytvára nový (takéto zaobchádzanie je potrebné z dôvodu bezpečnosti).



4. 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

