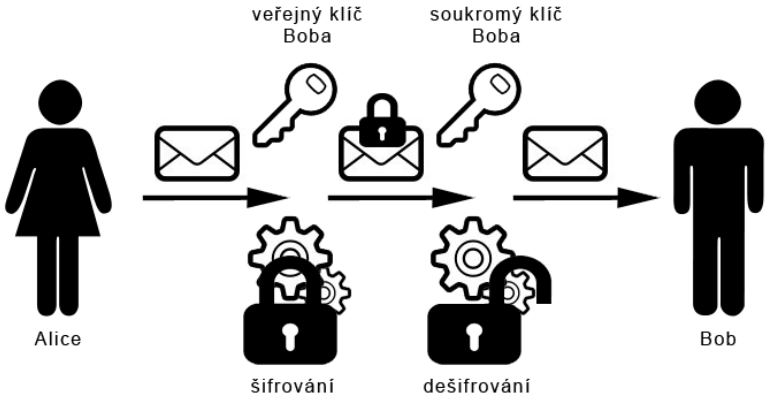
SPRÁVA ŽELEZNIC

Šifrování e-mailových zpráv pomocí PGP v aplikacích MS Outlook a Mozilla Thunderbird

Tento dokument představuje jednoduchý ilustrativní návod pro realizaci šifrované e-mailové komunikace s týmem CSIRT SZ Správy železnic, státní organizace. Prezentuje šifrování, dešifrování a podepisování e-mailových zpráv pomocí PGP klíčového páru s využitím dvou nejpoužívanějších aplikací MS Outlook a Mozilla Thunderbird.

Pro šifrování, dešifrování a digitální podepisování e-mailových zpráv využívá tým CSIRT SZ PGP klíče založené na algoritmu RSA (4096 b).

Algoritmus RSA patří mezi asymetrické šifrovací algoritmy, jejichž principem je existence **dvojice vzájemně matematicky provázaných klíčů** (veřejný a soukromý klíč). **Veřejný klíč slouží k šifrování a jeho výstupem je zašifrovaná zpráva,** kterou je možné **dešifrovat pouze pomocí odpovídajícího soukromého klíče** (viz následující obrázek). **Soukromý klíč je současně určen k podepisování zpráv, čímž je zaručena jejich autenticita.**



Alice šifruje e-mail Bobovi

Podrobnější informace o algoritmu RSA najdete například zde.

Šifrované e-mailové zprávy je vhodné použít v případě, že odesílatel si přeje zasílat informace citlivého charakteru a nechce, aby k nim měl přístup někdo jiný než osoba, které je zpráva určena. Zde na webových stránkách **CSIRT SZ je umístěn veřejný klíč**, který je určen jak pro běžnou komunikaci s naším týmem, a to na e-mailovou adresu

soc@spravazeleznic.cz**, tak veřejný PGP klíč slouží i pro hlášení incidentů, citlivých dat a informací** na e-mailovou adresu soc@spravazeleznic.cz**.**

Poznámka
Pro ilustrativní příklad byl využit veřejný PGP klíč Národního centra kybernetické bezpečnosti.

Instalace PGP pro MS Outlook

Jednou možností, jak šifrovat pomocí PGP v aplikaci MS Outlook, je instalace balíčku **GPG4Win** s přiloženým pluginem **GpgOL.** GPG4Win je možné stáhnout **zde.** Balíček obsahuje následující aplikace (**tučně jsou vyznačeny aplikace a pluginy, které je potřeba určitě nainstalovat**):

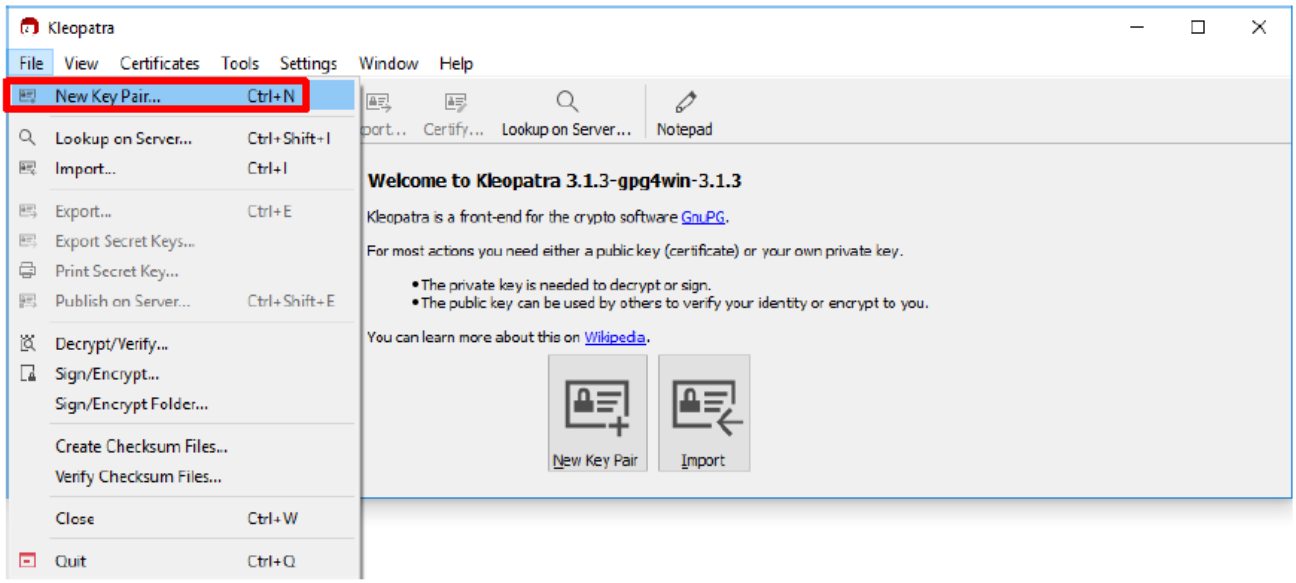
- **GnuPG – šifrovací nástroj**
- **Kleopatra – správce klíčů pro OpenPGP a X.509 (S/MIME)**
- GPA – alternativní správce klíčů
- GpgEX – plugin pro Microsoft Explorer
- **GpgOL – plugin pro MS Outlook 2010/2013/2016 (32 i 64 bit verze)**
- Compendium – dokumentace v angličtině a němčině

Další možností je **šifrovat a podepisovat** (resp. dešifrovat a ověřovat) soubory v **externí aplikaci** (například Kleopatra), a ty pak připojit jako přílohu nešifrovaného e-mailu.

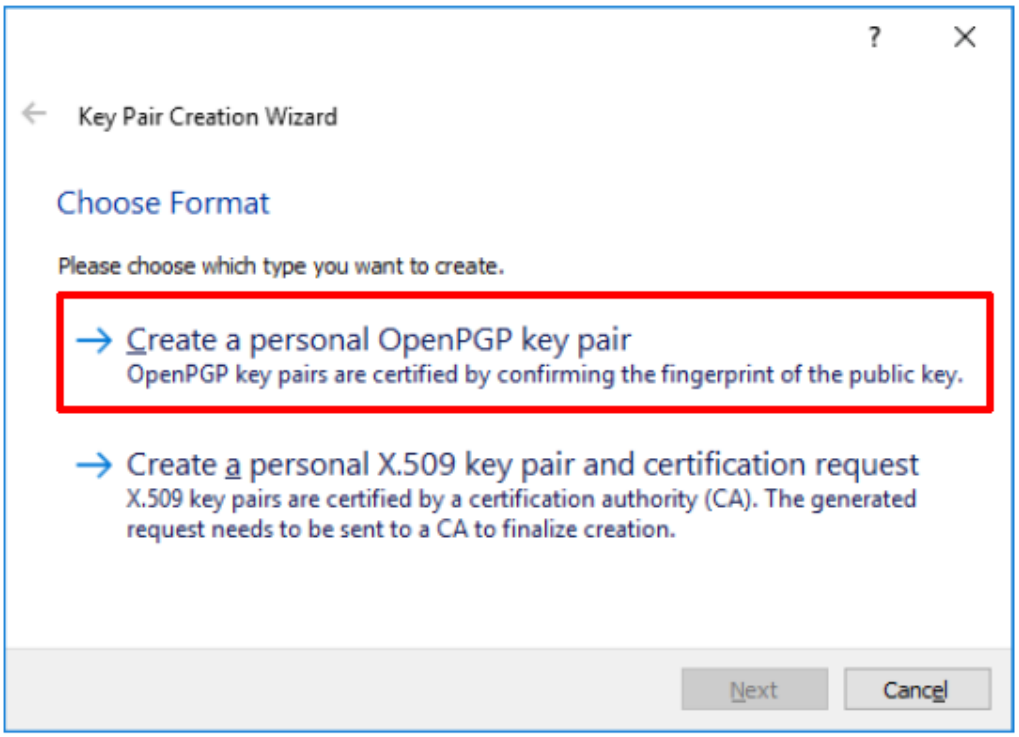
Po nainstalování potřebných pluginů a aplikací z balíčku GPG4Win **spusťte aplikaci Kleopatra.** V případě, že již máte svůj PGP klíč, můžete následující krok „Vytvoření vlastního PGP certifikátu „přeskočit.

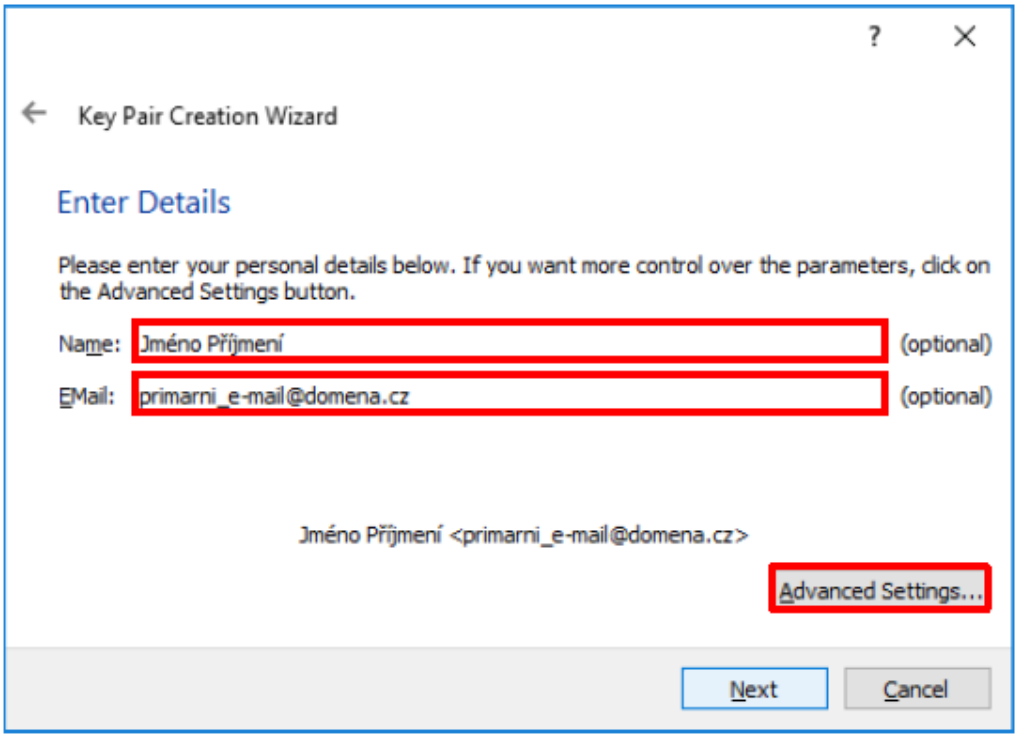
Vytvoření vlastního PGP certifikátu v aplikaci Kleopatra

Pro **vytvoření vlastního PGP certifikátu** (veřejného a soukromého PGP klíče) můžete zvolit následující postup: ***„File" -> „New certificate..."*.**



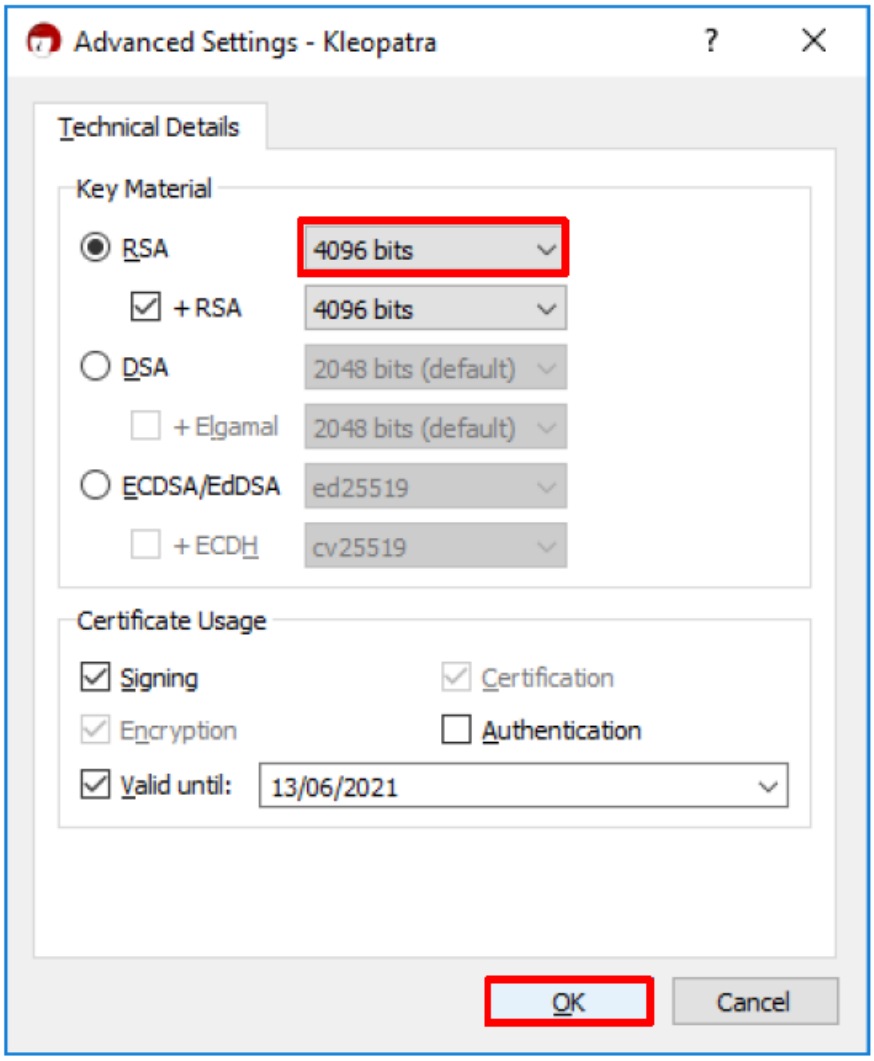
Následně zvolíte ***„Create a personal OpenPGP key pair"*** a v dalším okně vyplníte odpovídající údaje.



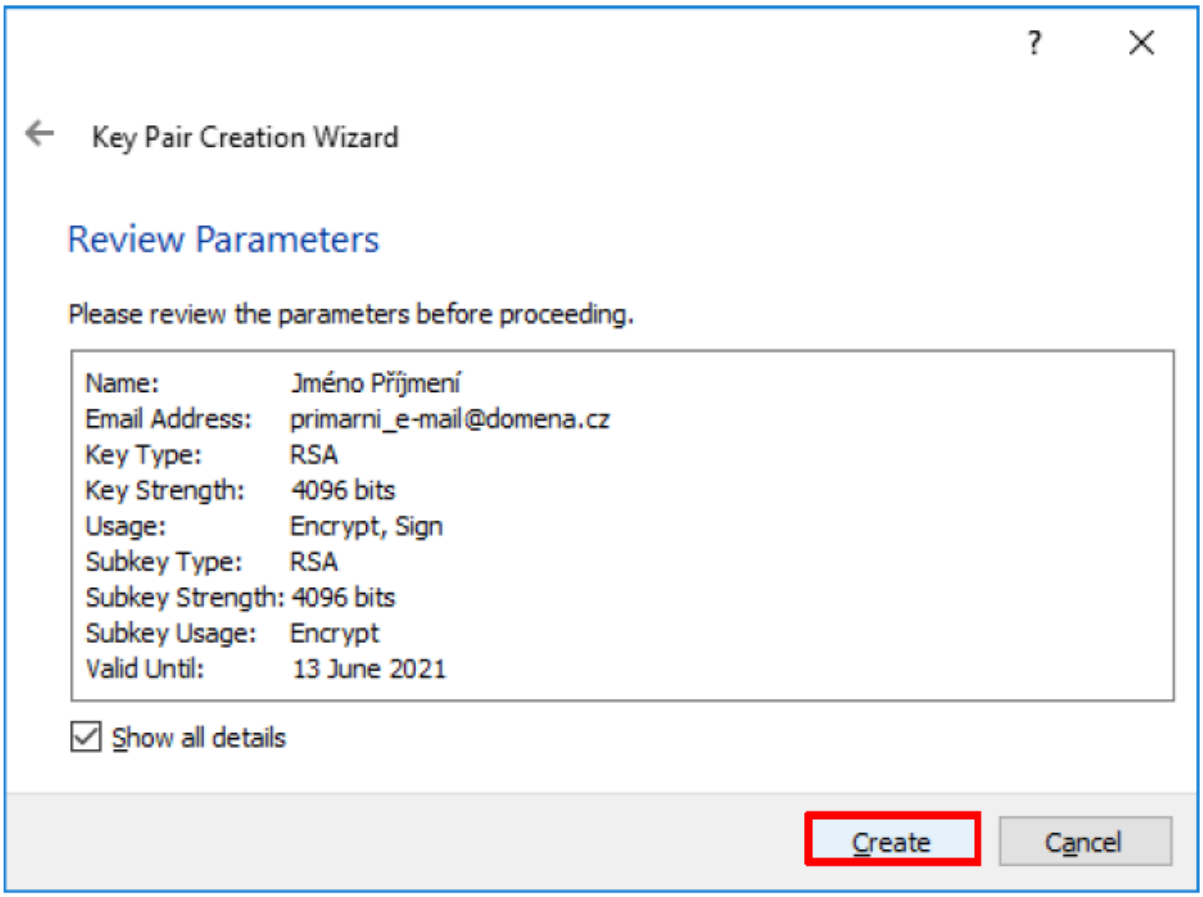


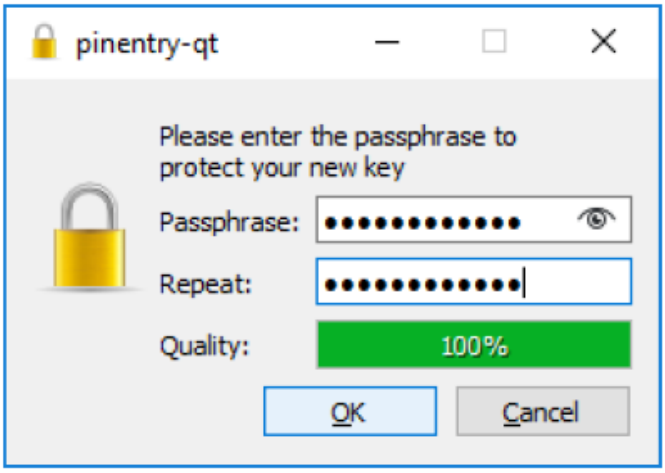
Posléze stiskněte tlačítko **„Advanced Setting..."**.

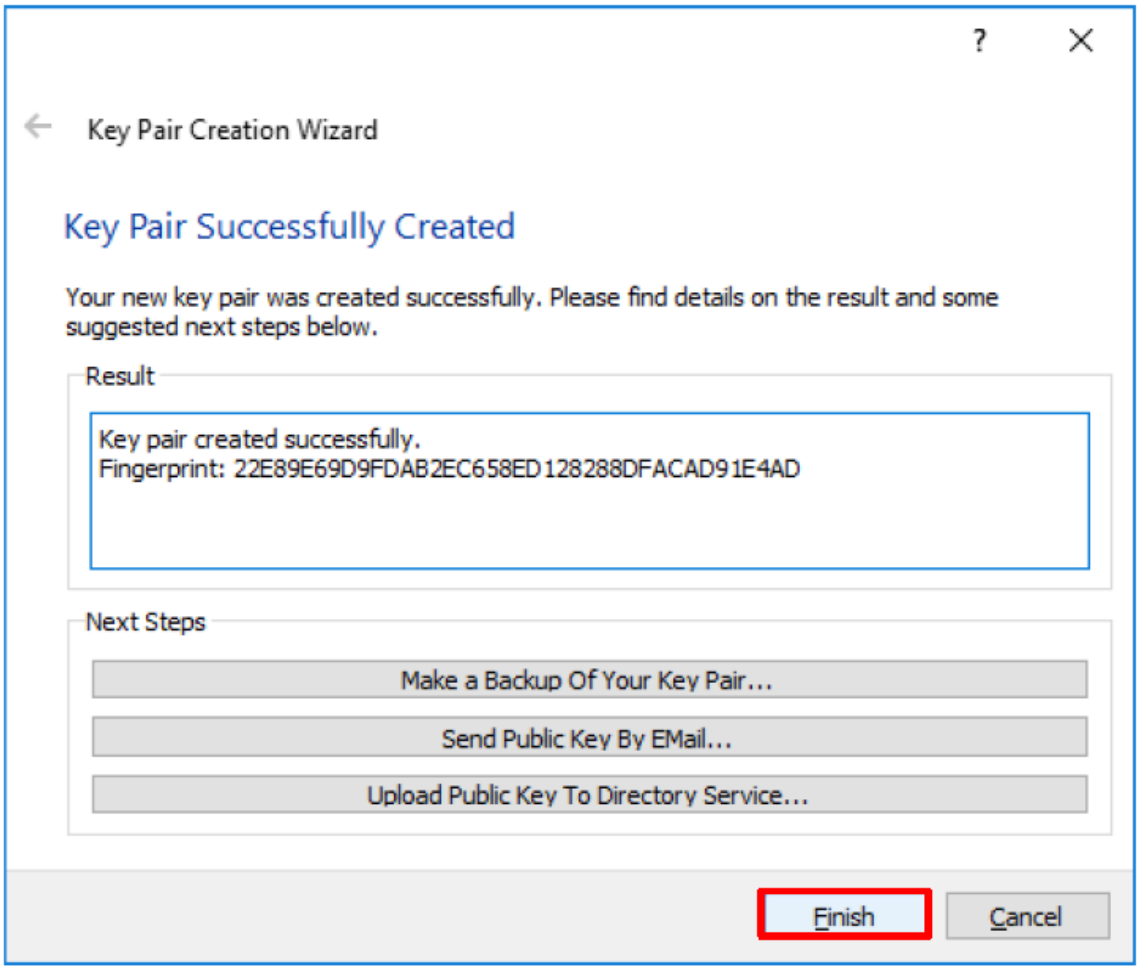
Zvyšte hodnotu RSA na 4096 bits, případně můžete podle potřeby nastavit délku platnosti klíče. **Potvrdíte** stisknutím ***„OK"*** a pokračujte v okně Enter Details **stiskem *„Next".***



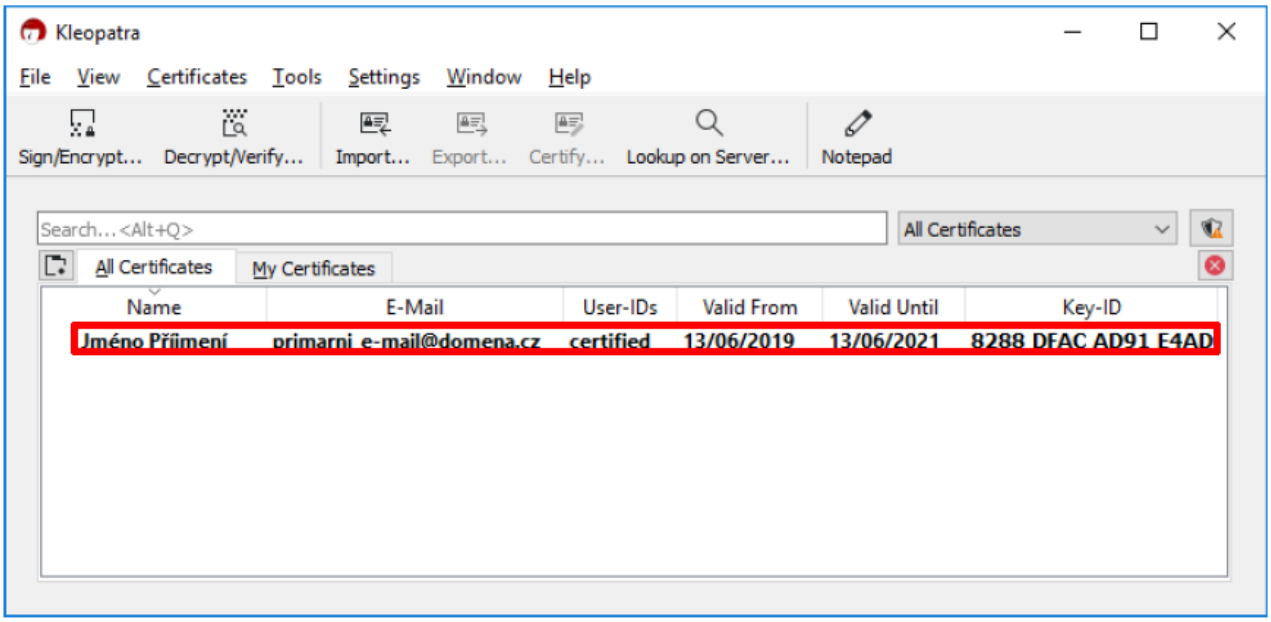
Zkontrolujte zadané parametry a **stiskem *„Create"*** začněte generovat samotné klíče. V průběhu budete **vyzváni k zadání a potvrzení hesla,** které slouží jako **autentizace vlastníka certifikátu,** čímž se chráníte před jeho případným odcizením. **Při tvorbě bezpečného hesla je vhodné aplikovat pravidla best-practices. Jak na bezpečné heslo se můžete podívat i zde.**


Key Pair Creation Wizard
Review Parameters
Please review the parameters before proceeding.
Name: Jméno Příjmení
Email Address: primarni_e-mail@domena.cz
Key Type: RSA
Key Strength: 4096 bits
Usage: Encrypt, Sign
Subkey Type: RSA
Subkey Strength: 4096 bits
Subkey Usage: Encrypt
Valid Until: 13 June 2021
Show all details
Create
Cancel


pinentry-qt
Please enter the passphrase to protect your new key
Passphrase:
Repeat:
Quality:
100%
OK
Cancel



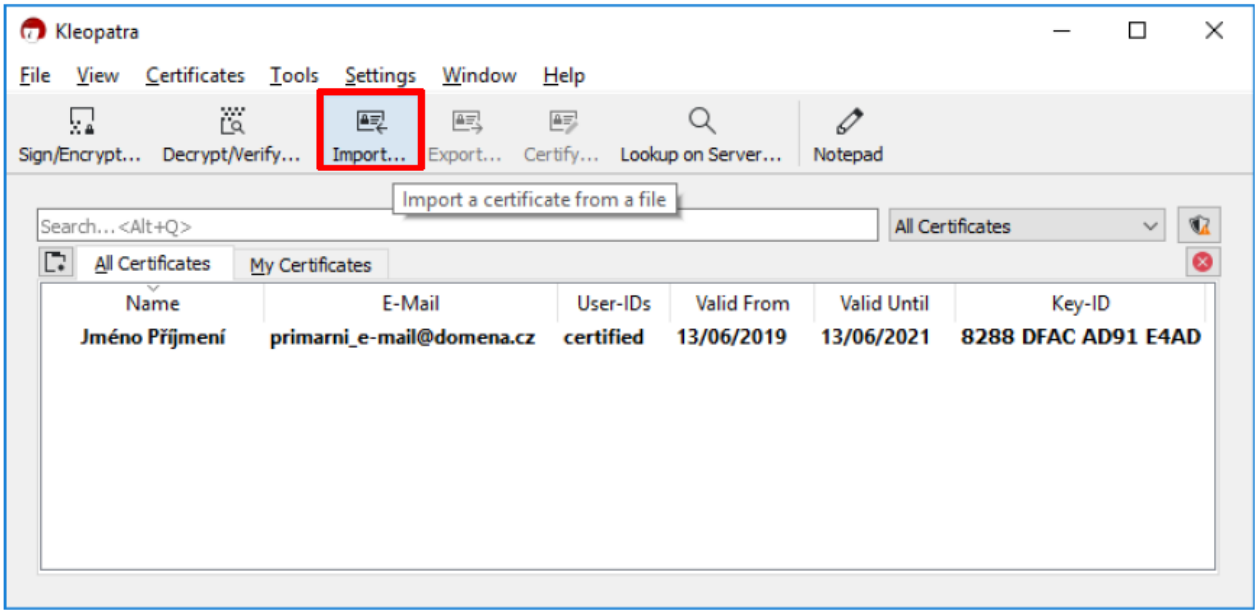
Po dokončení procesu generování párů klíčů máte **několik možností, jak si je uložit** a **stiskněte** tlačítko **„Finish".**



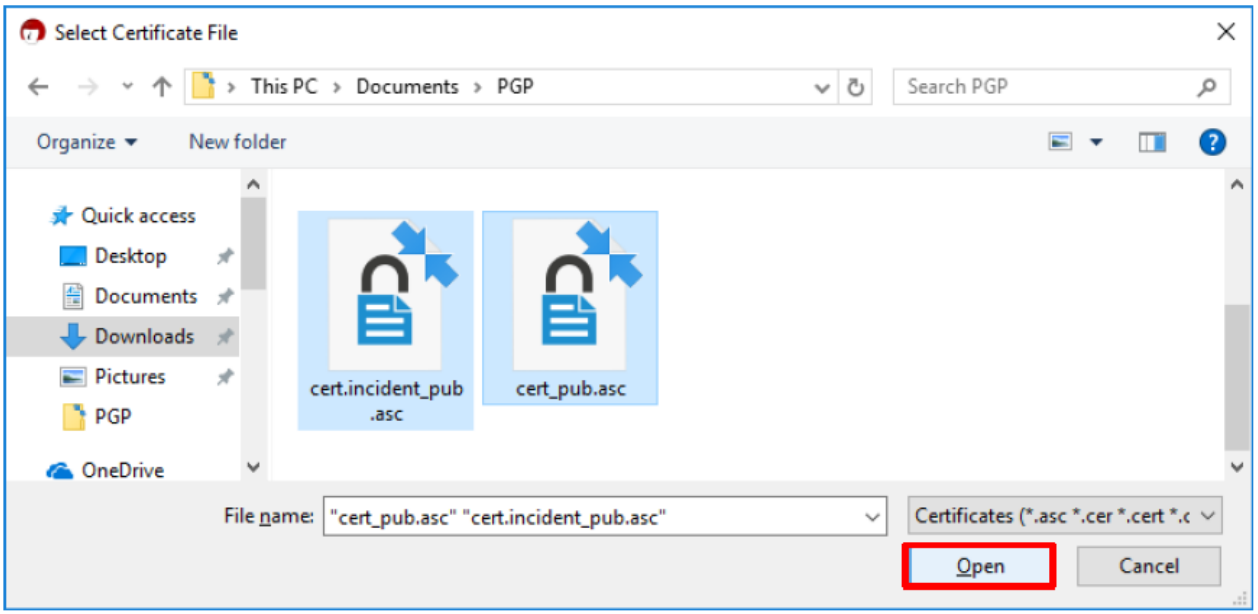
Jestliže jste zadali všechno správně, měl by se v programu Kleopatra objevit Váš nově vytvořený klíčový pár, obsahující soukromý a veřejný klíč.

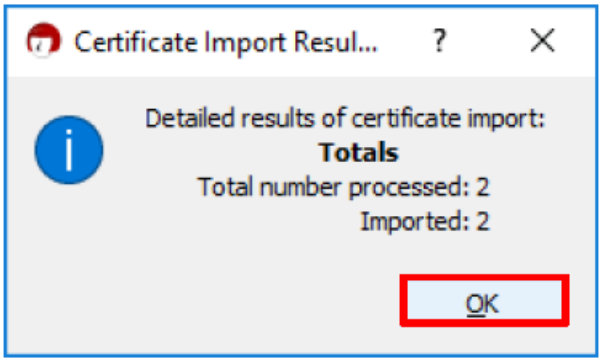
Import PGP certifikátů do aplikace Kleopatra

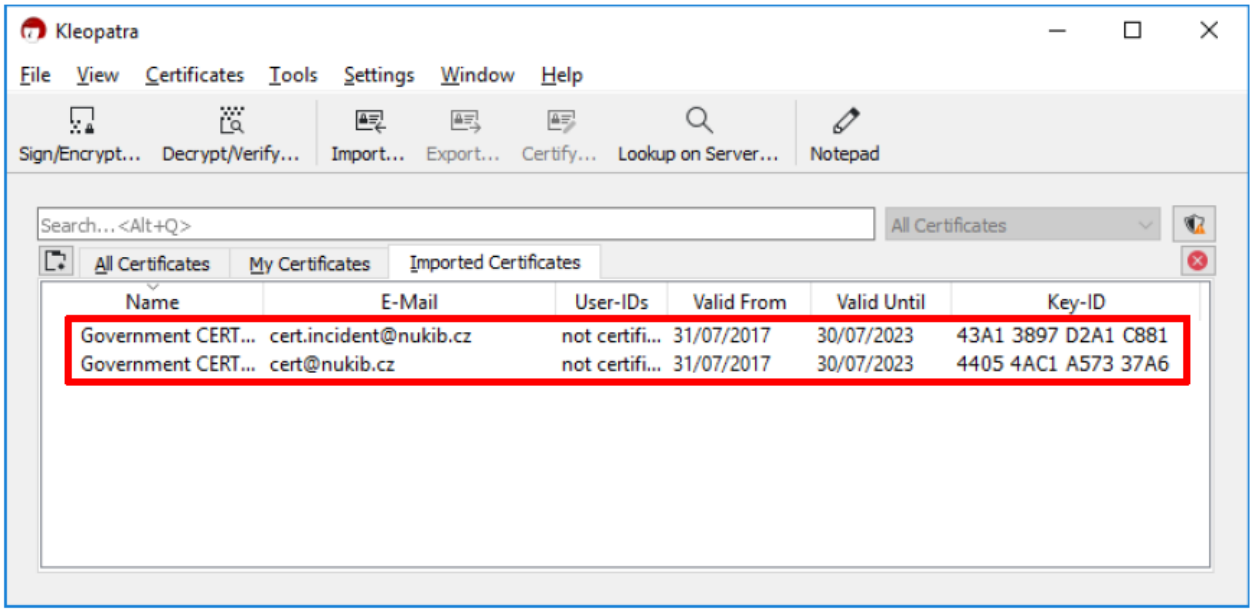
Jste-li již majitelem vlastního páru PGP klíčů, můžete je jednoduše naimportovat ***„File" -> „Import..."***. Dále je potřeba **naimportovat veřejný PGP klíč příjemce**, kterým je v našem případě **CSIRT SZ**. **Tyto veřejné klíče lze stáhnout na našich webových stránkách www.spravazeleznic.cz, viz výše.**



Pro import veřejného klíče příjemce se postupuje obdobně, zvolíte ***„File" -> „Import..."***, nebo klikněte na stejnojmennou ikonku pod hlavním menu aplikace a vyberete příslušné soubory. **Potvrďte** stisknutím ***„Otevřít".*** Nakonec v malém okně **Certificate Import Resolution stiskněte *„OK".***



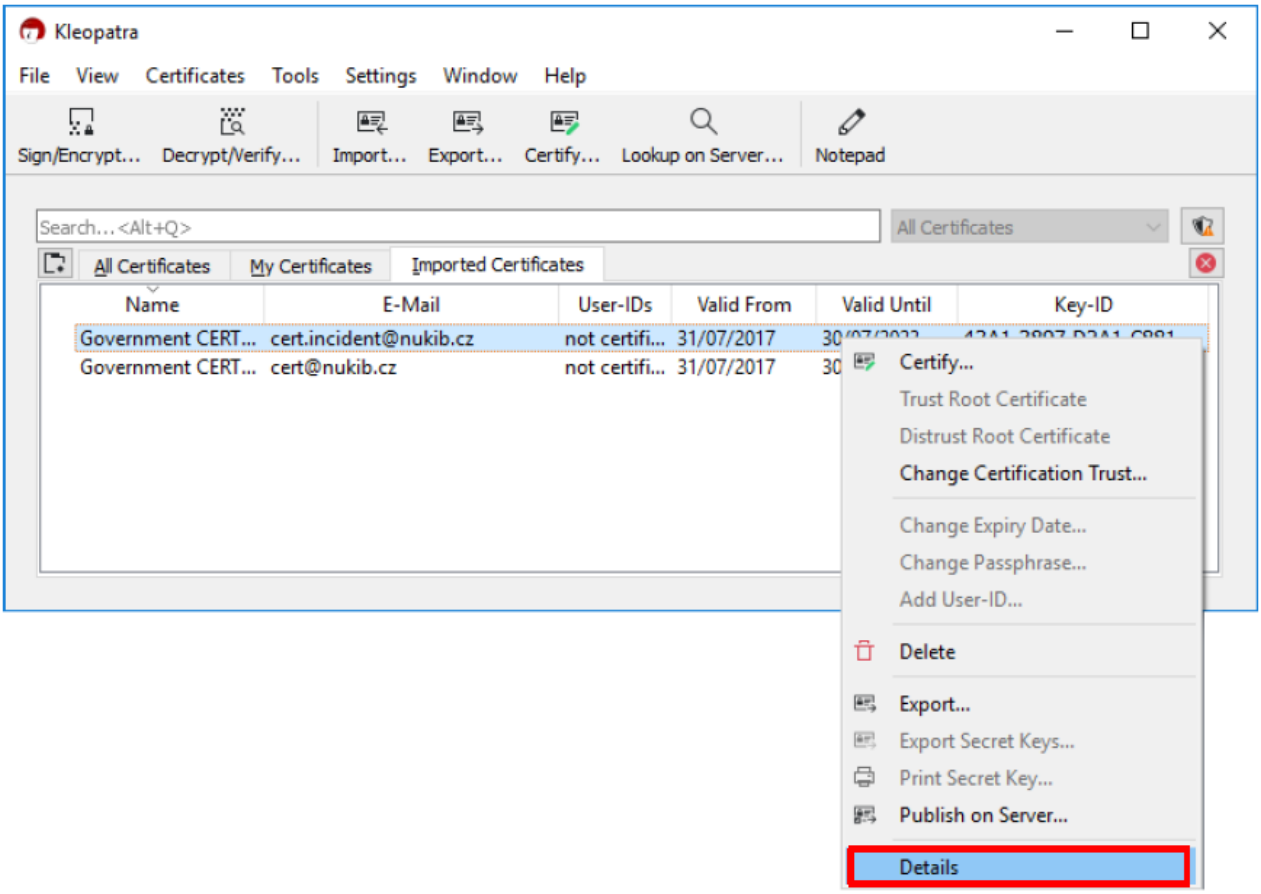




V tuto chvíli byste měli mít v aplikaci Kleopatra v pořádku naimportovány veřejné klíče.

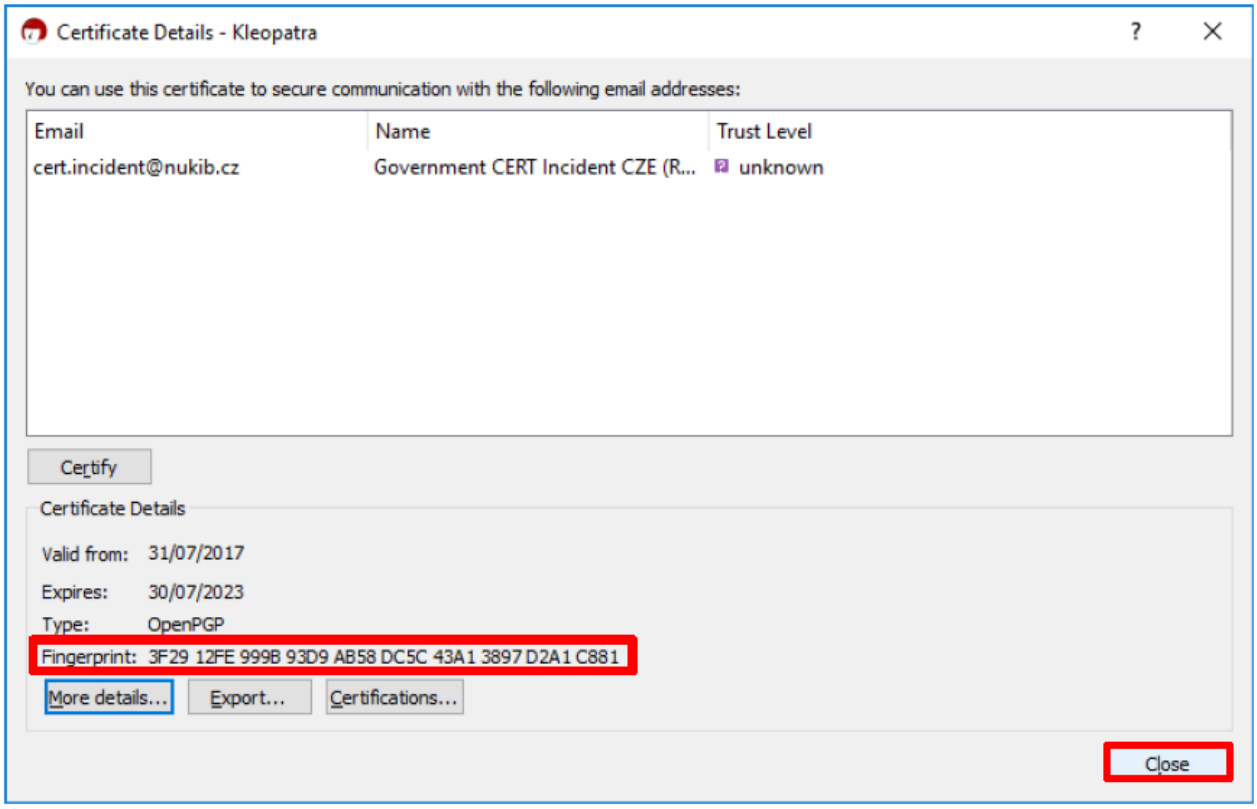
Kontrola PGP certifikátů

Po importování potřebného PGP klíče (viz přiložený obrázek) je potřeba zkontrolovat **otisk klíče neboli *„fingerprint*". Toto ověření se provede **kliknutím pravým tlačítkem** na **příslušný certifikát** a **kliknutím** na položku ***„Details*".**



V poli *„fingerprint*" by se měly nacházet tyto hodnoty:

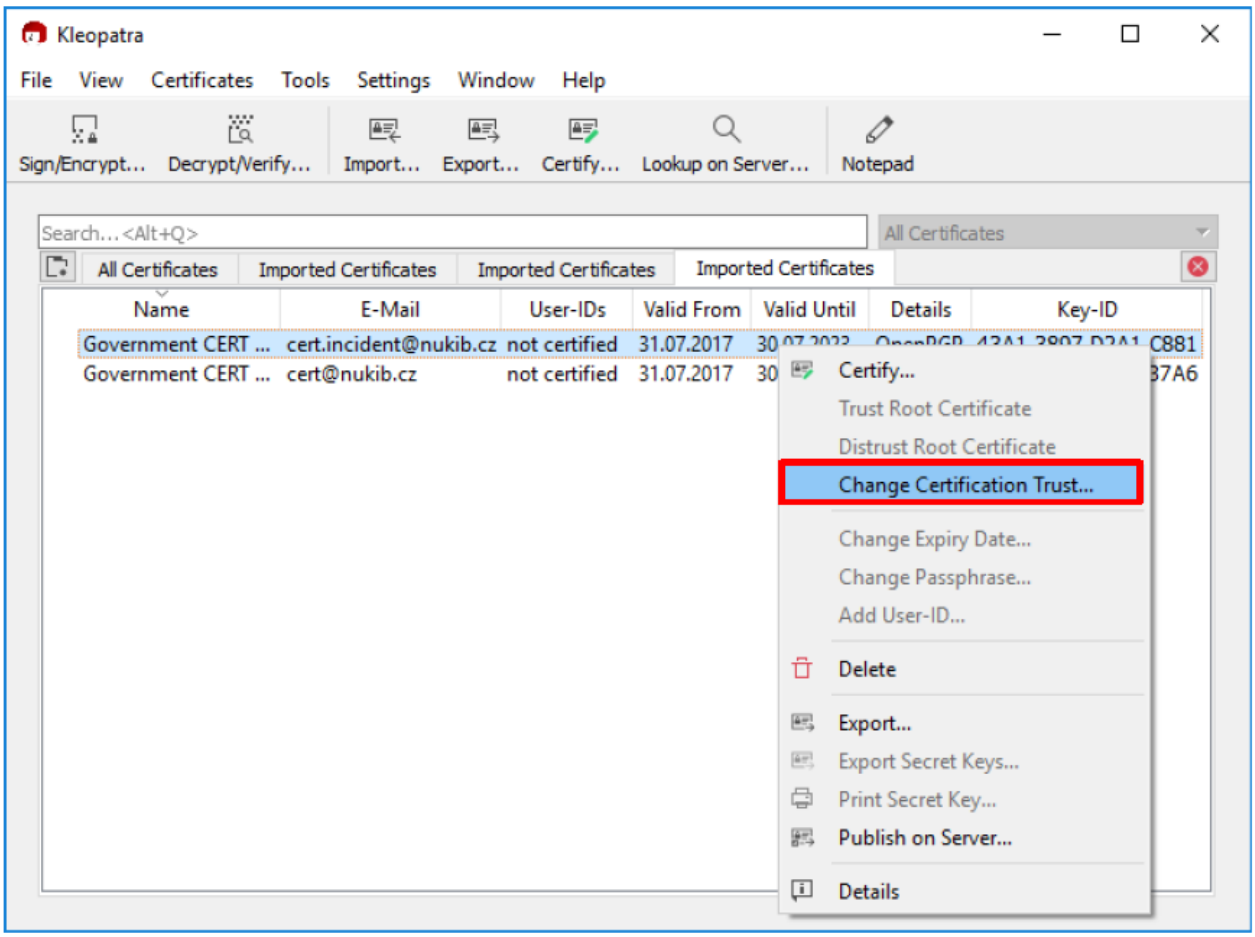
E1A5 18B9 95FB 2E00 2727 9566 D7DD CFAA 3C5D 46E1 pro e-mail soc@spravazeleznic.cz

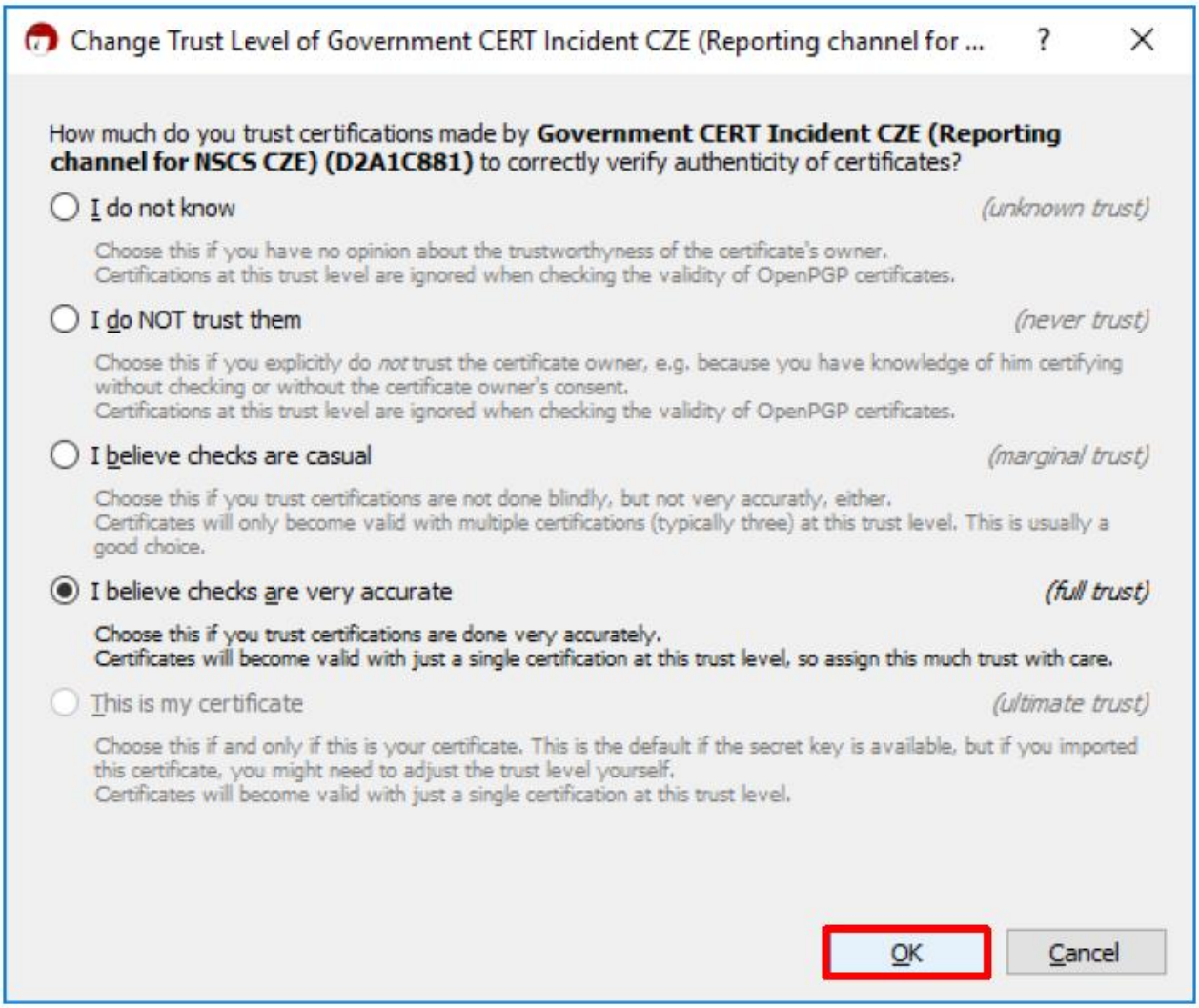


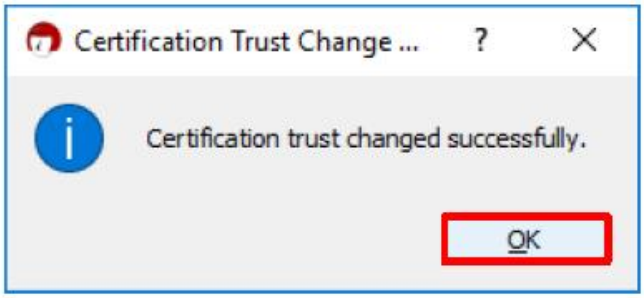
Pokud tyto hodnoty souhlasí, okno zavřete stiskem tlačítka *„Close*".

Nastavení důvěryhodnosti certifikátů

Po ověření je nutné nastavit u certifikátu **důvěryhodnost**. To provedete tak, že pravým tlačítkem myši **kliknete na každý jednotlivý certifikát a nastavíme parametr *„Change Certification Trust"* na patřičnou hodnotu**. Pokud certifikátu důvěřujete, **nastavte** úroveň důvěry na ***„full trust"***, tedy ***„I believe checks are very accurate"***. Následně **dvakrát potvrďte** stiskem na tlačítka ***„OK"*.**



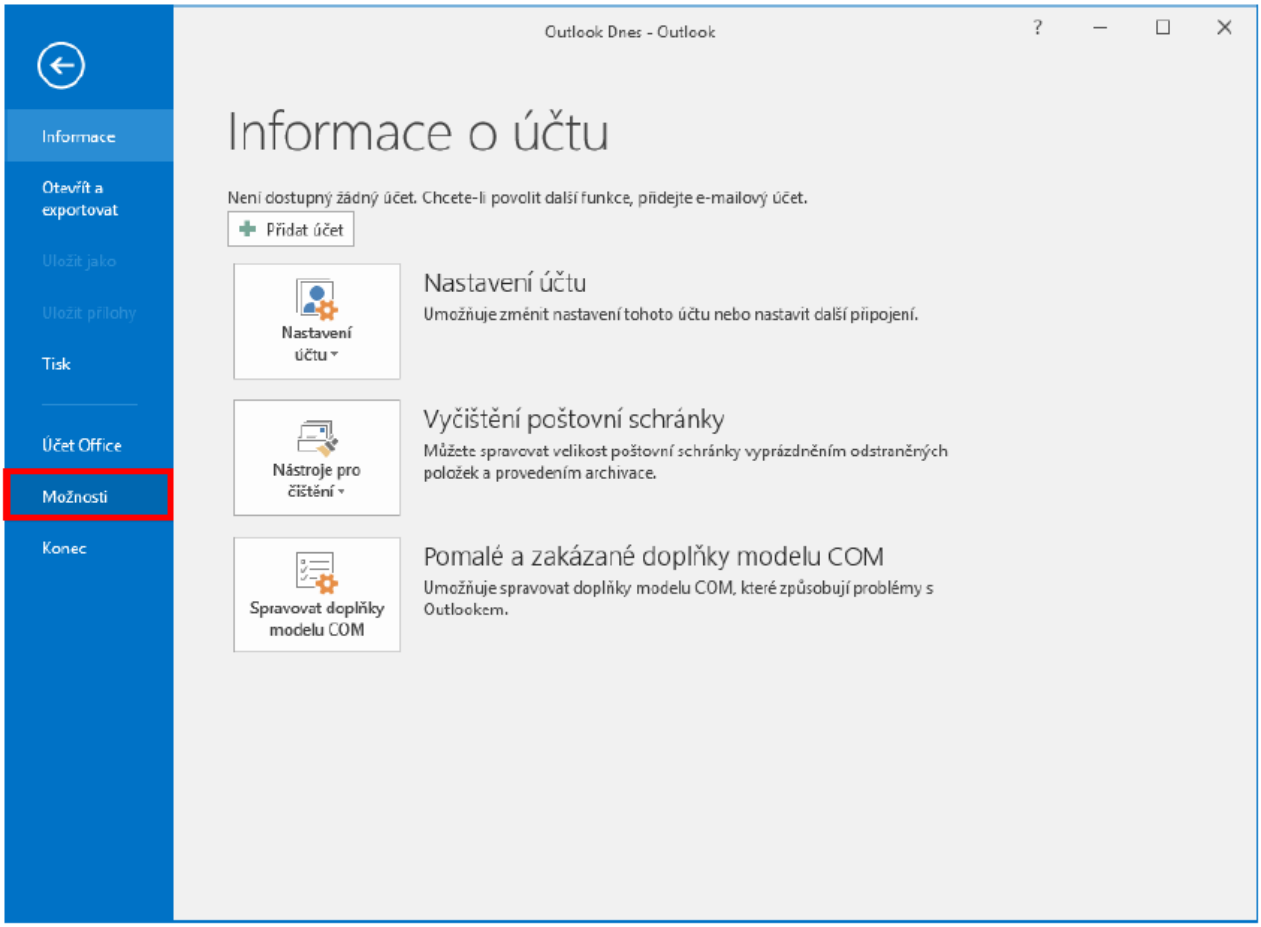




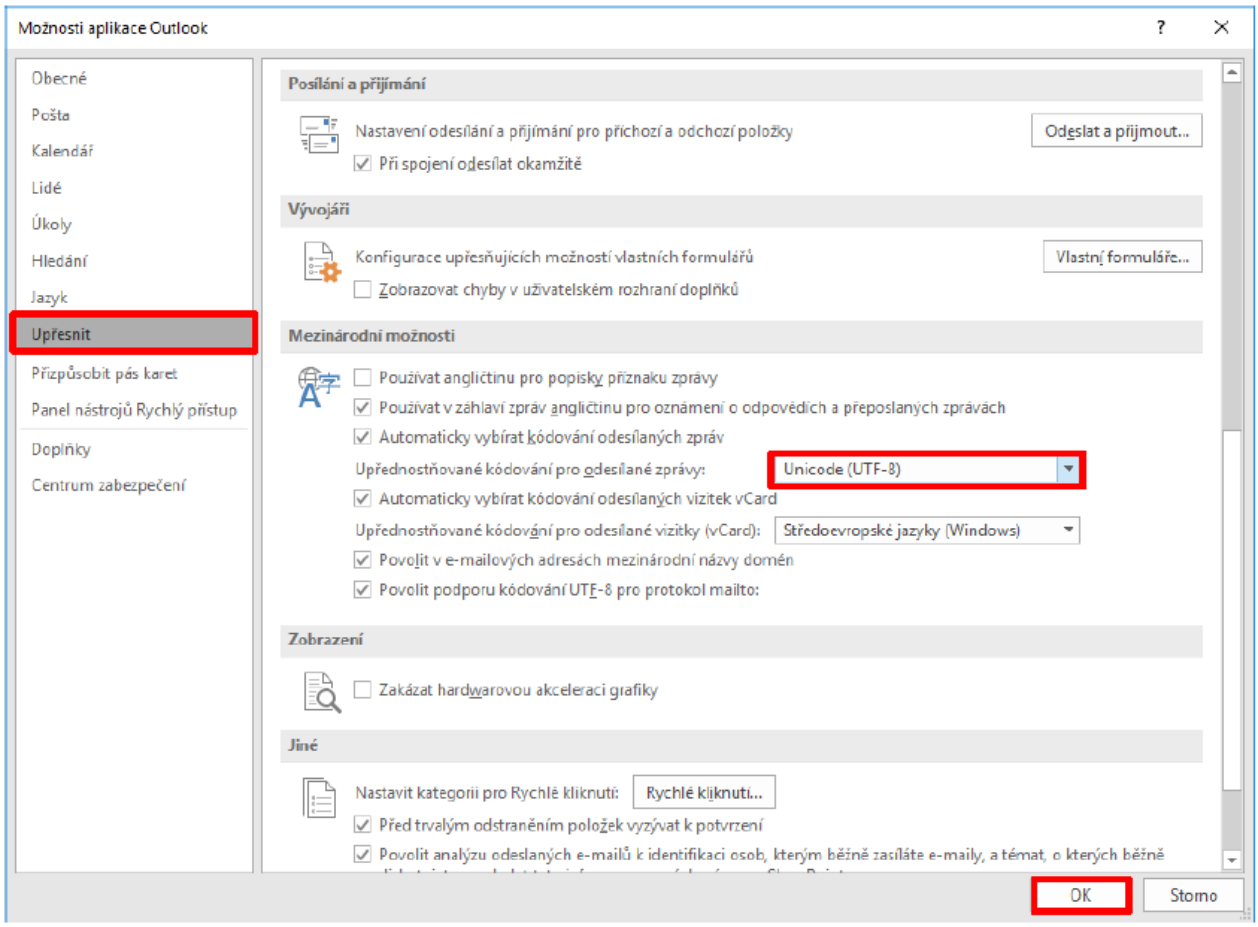
Aplikaci Kleopatra lze nyní vypnout.

Nastavení kódování pro odesílané zprávy

Nyní ještě zbývá v aplikaci MS Outlook **nastavit správné kódování e-mailu** pro korektní zobrazení, které provedete následovně: v záložce ***„Soubor"*** **zvolte** položku ***„Možnosti"*** a v této vyberte záložku ***„Upřesnit"*.**

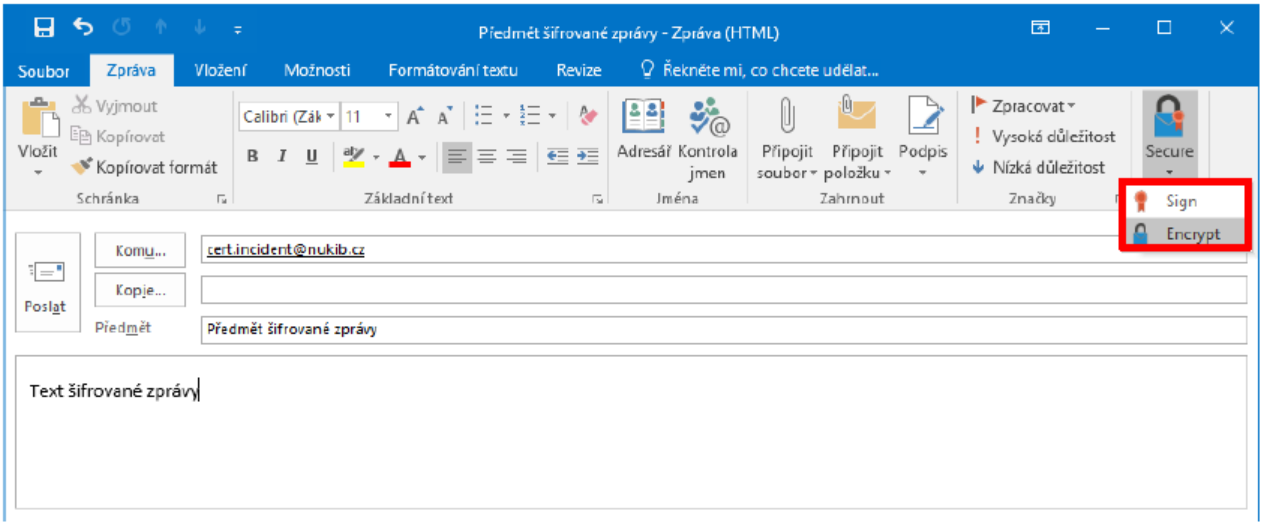


V záložce ***„Upřesnit"*** je v části ***„Mezinárodní možnosti"*** **nutno změnit** položku ***„Upřednostňované kódování pro odesílané zprávy"*.** Zde **nastavte** hodnotu ***„Unicode (UTF-8)"*.**


Možnosti aplikace Outlook
Obecné
Pošta
Kalendář
Lidé
Úkoly
Hledání
Jazyk
Upřesnit
Přizpůsobit pás karet
Panel nástrojů Rychlý přístup
Doplňky
Centrum zabezpečení
Posílání a přijímání
Nastavení odesílání a přijímání pro příchozí a odchozí položky
Odeslat a přijmout...
Při spojení odesílat okamžitě
Vývojáři
Konfigurace upřesňujících možností vlastních formulářů
Vlastní formuláře...
Zobrazovat chyby v uživatelském rozhraní doplňků
Mezinárodní možnosti
Používat angličtinu pro popisky příznaku zprávy
Používat v záhlaví zpráv angličtinu pro oznámení o odpovědích a přeposlaných zprávách
Automaticky vybírat kódování odesílaných zpráv
Upřednostňované kódování pro odesílané zprávy:
Unicode (UTF-8)
Automaticky vybírat kódování odesílaných vizitek vCard
Upřednostňované kódování pro odesílané vizitky (vCard):
Středoevropské jazyky (Windows)
Povolit v e-mailových adresách mezinárodní názvy domén
Povolit podporu kódování UTF-8 pro protokol mailto:
Zobrazení
Zakázat hardwarovou akceleraci grafiky
Jiné
Nastavit kategorii pro Rychlé kliknutí:
Rychlé kliknutí...
Před trvalým odstraněním položek vyzývat k potvrzení
OK
Storno

Šifrování e-mailové zprávy v MS Outlook

Způsob šifrování e-mailu v aplikaci MS Outlook je pak následující: v záložce ***„Domů"*** zvolte položku ***„Nový e-mail"***, do kterého **vyplňte standardní údaje** jako **e-mailovou adresu příjemce, předmět a obsah zprávy**. **Pro obousměrnou šifrovanou komunikaci vložíte** do přílohy svůj **veřejný PGP klíč**. To provedete buď v záložce ***„Zpráva"*** **->** ***„Zahrnout"*** **->** ***„Připojit Soubor"*** a vyberete **soubor s veřejným klíčem. Možnost podepisovat či šifrovat zprávy** lze zvolit v **záložce *„GpgOL"***, kde volbou ***„Sign"*** **odchozí zprávu podepíšete** a volbou ***„Encrypt"*** **zašifrujete**.

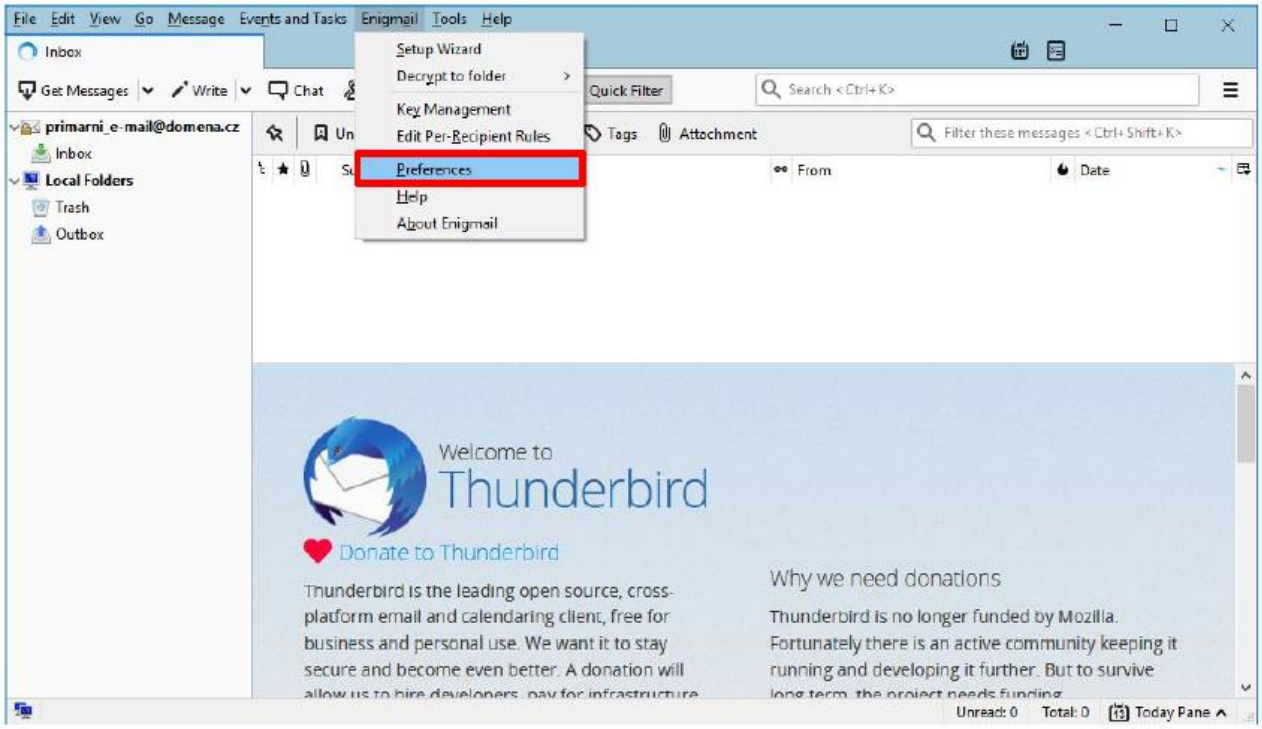


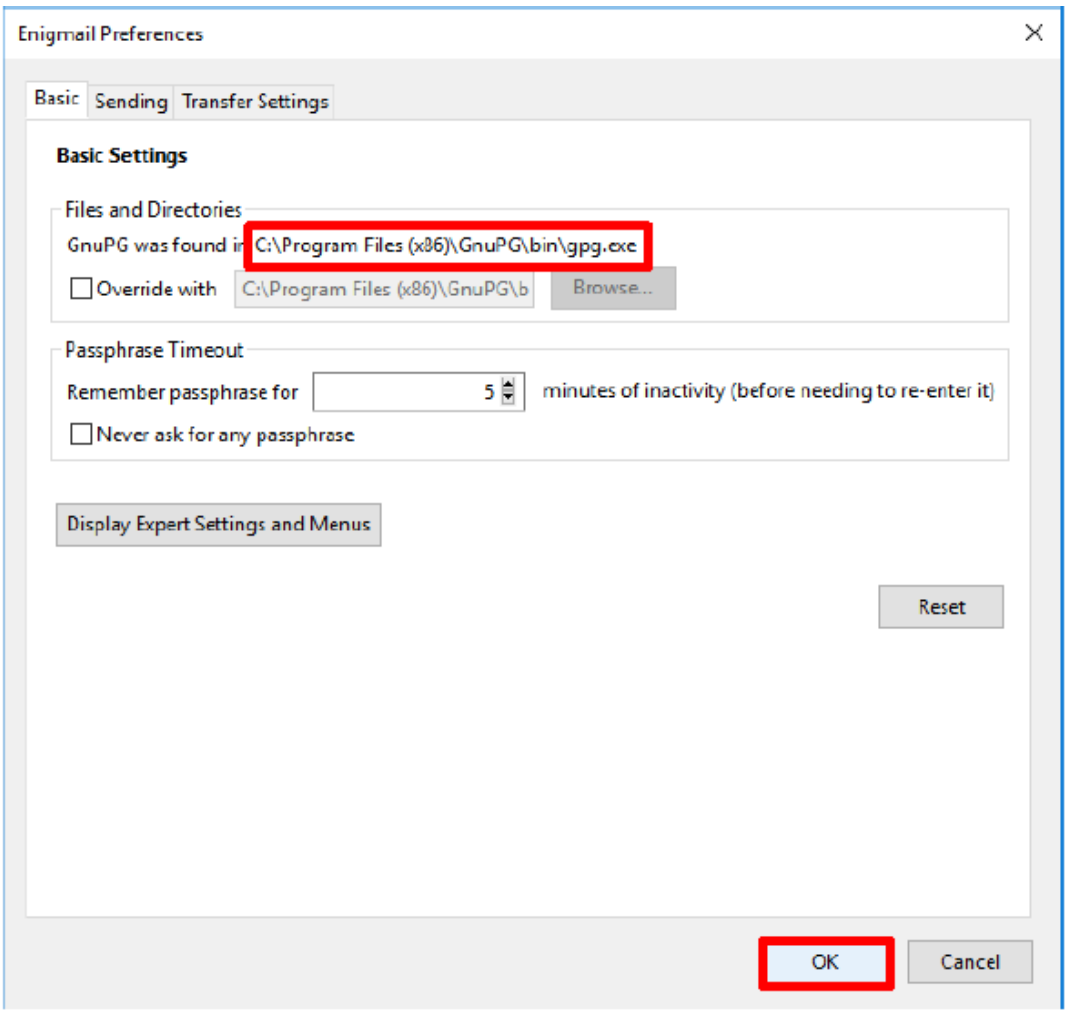
Nyní je již možno e-mail odeslat. Pokud byla zvolena **možnost *„Sign"***, bude **před jeho odesláním požádáno o zadání hesla** od Vašeho **soukromého klíče**. V případě, že databáze v aplikaci Kleopatra neobsahuje veřejný klíč odpovídající e-mailové adrese příjemce, budete před odesláním vyzváni k výběru odpovídajícího klíče.

Instalace PGP pro Mozilla Thunderbird

Pro funkční šifrování e-mailové komunikace pomocí PGP je **nezbytné nainstalovat e-mailového klienta Mozilla Thunderbird** a **provést nastavení svého e-mailového účtu**, ze kterého budete odesílat šifrované e-maily. Dále je ještě **potřeba nainstalovat aplikaci GnuPG** (například z balíčku GPG4Win – viz výše) a v **Mozilla Thunderbird plugin Enigmail**. Druhý zmiňovaný **doplněk nainstalujete následným způsobem**: přejděte do ***„Tools"* -> *„Add-ons"* -> *„Extensions"*** *(Nástroje -> Doplňky -> Rozšíření)* a zde dejte **vyhledat plugin Enigmail**. Tento plugin nainstalujte a restartujte e-mailového klienta.

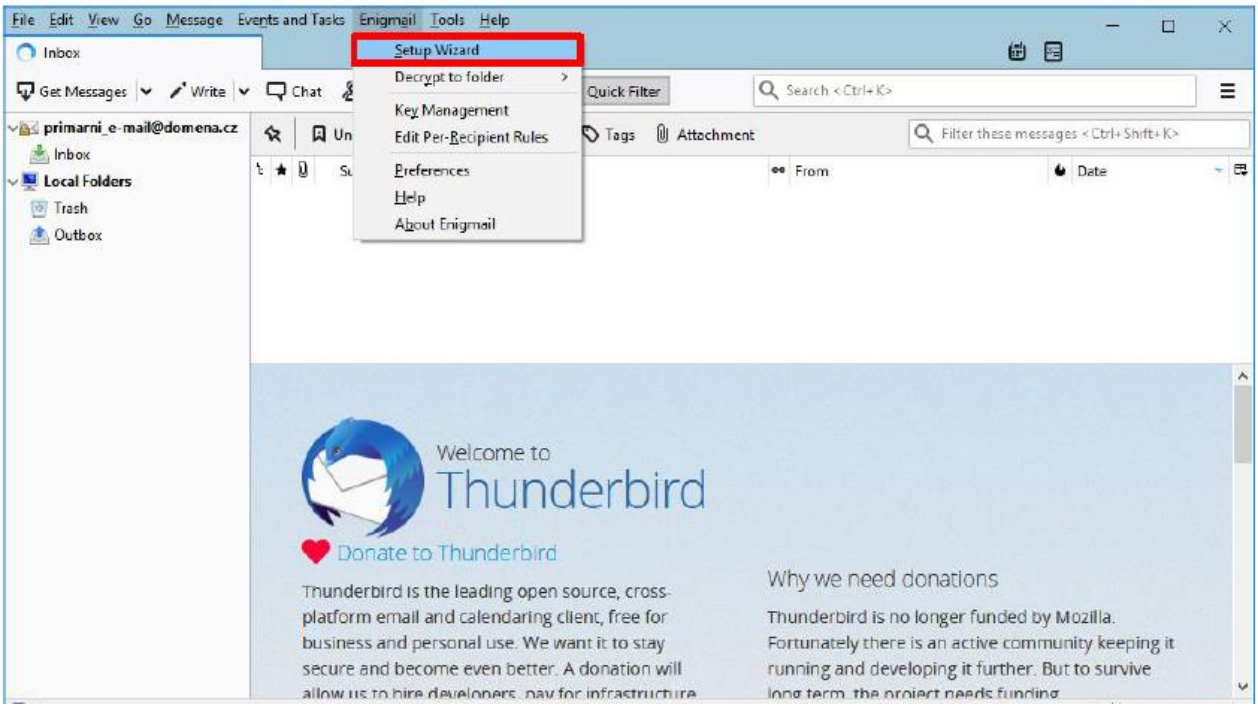
Po restartu se v liště s menu Mozilla Thunderbird objeví položka *„Enigmail"*. Tu **rozklikněte** a v položce ***„Preferences"*** *(Předvolby…)* v záložce ***„Basic"*** *(Základní)* zkontrolujte, zda se nastavila správná cesta k místu, kam jste nainstalovali aplikaci GnuPG.



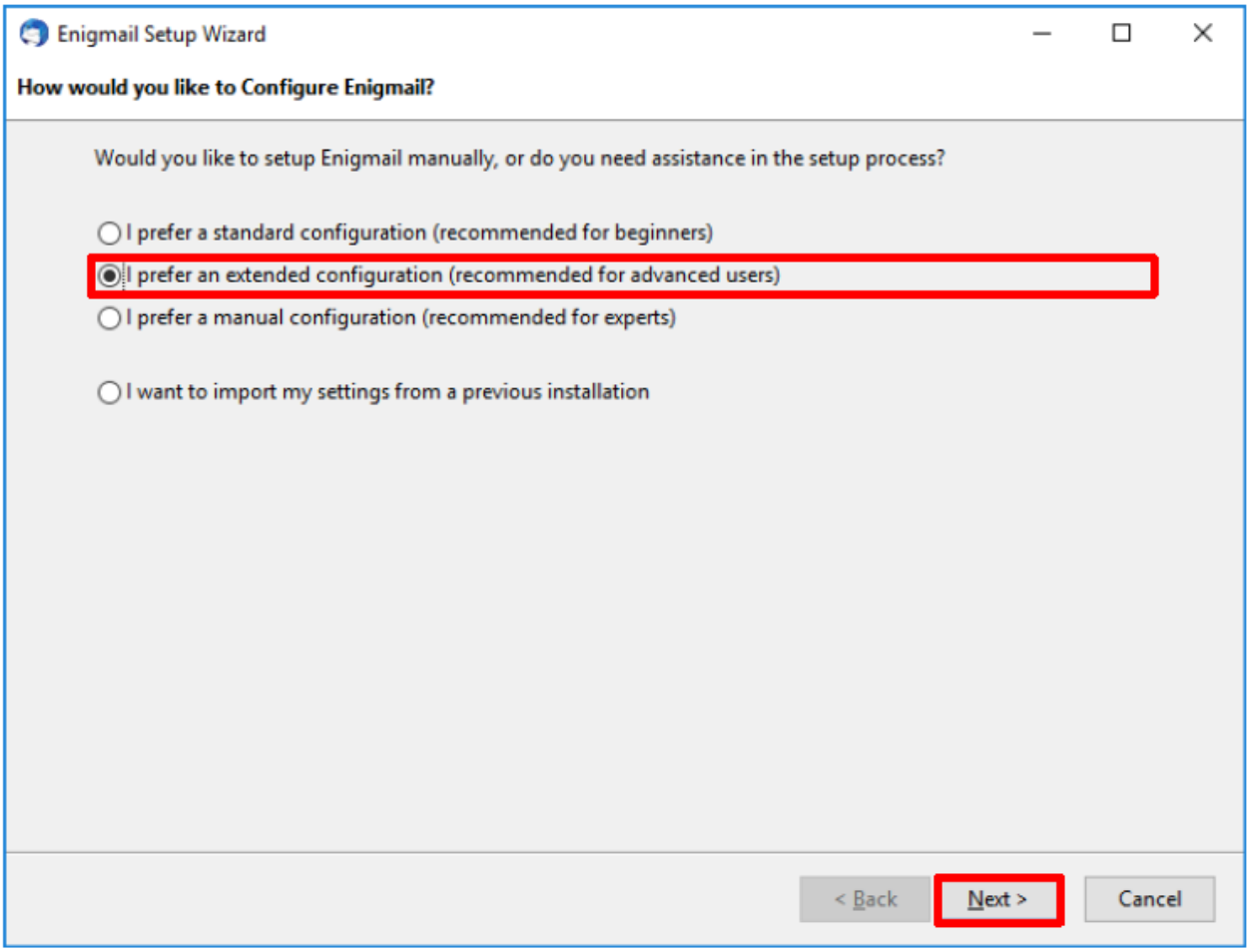


Pokud zde není uvedena žádná cesta, nebo je uvedena nesprávná cesta instalace aplikace, je nutno ji správně doplnit či opravit.

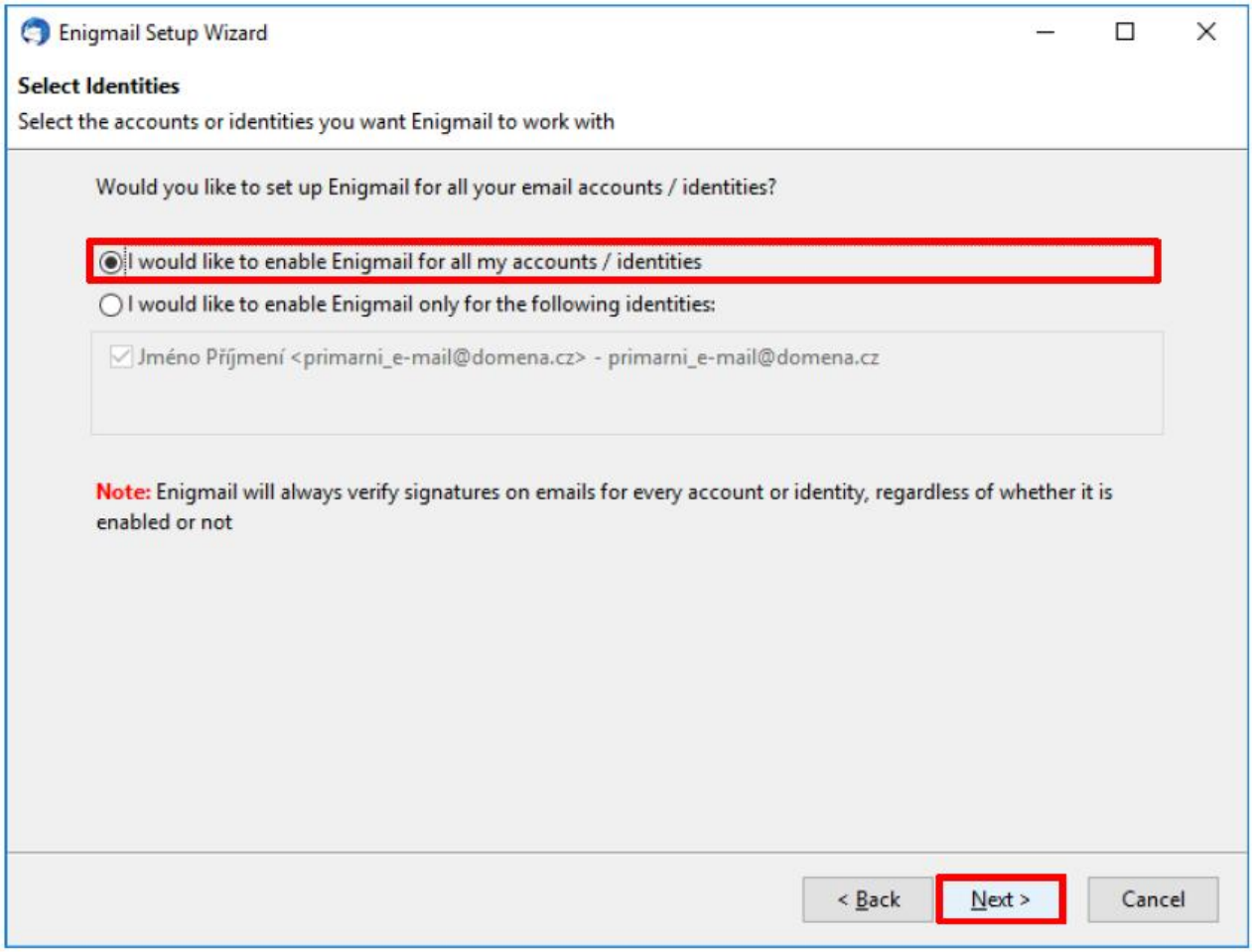
Nyní v menu ***„Enigmail"*** **zvolte** předposlední položku ***„Setup Wizard"*** (Průvodce nastavením)



V následujícím kroku zvolte položku ***„I prefer an extended configuration"***, tedy rozšířené nastavení, které nám umožní volbu existujících klíčů, či vytvoření nových. **Potvrďte** stiskem ***„Next"*** *(Další)*.



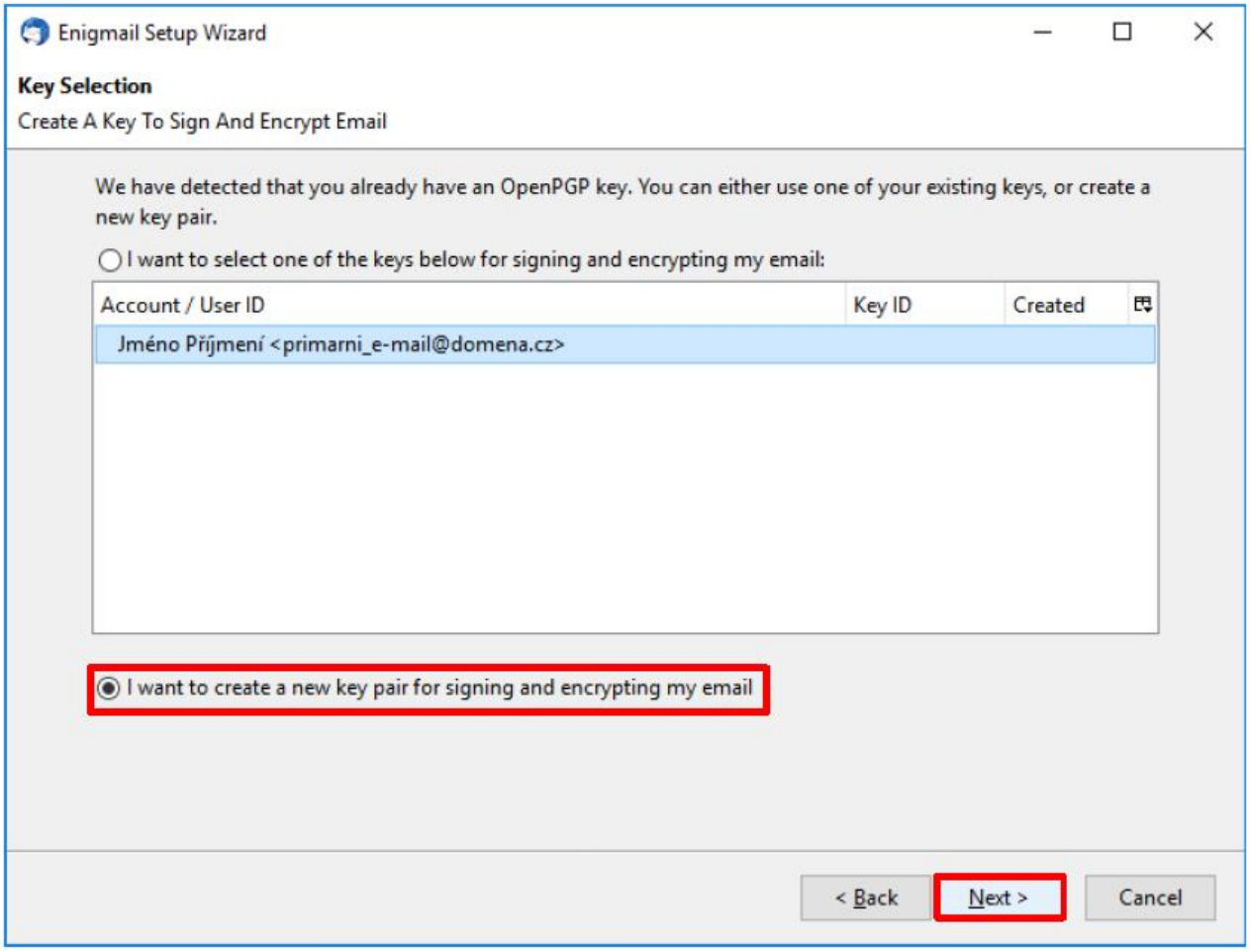
Dále je potřeba **zvolit, pro které Vaše e-mailové účty chcete používání PGP certifikátů nastavit.** Pokud používáte více účtů, lze vybrat, se kterými konkrétními identitami bude Enigmail pracovat. V případě, že používáte pouze jeden, nebo chcete **pravidla nastavit pro všechny e-mailové účty**, **vyberte** první položku ***„I would like to enable Enigmail for all my accounts / identities"***. **Potvrďte** stiskem ***„Next"*.**



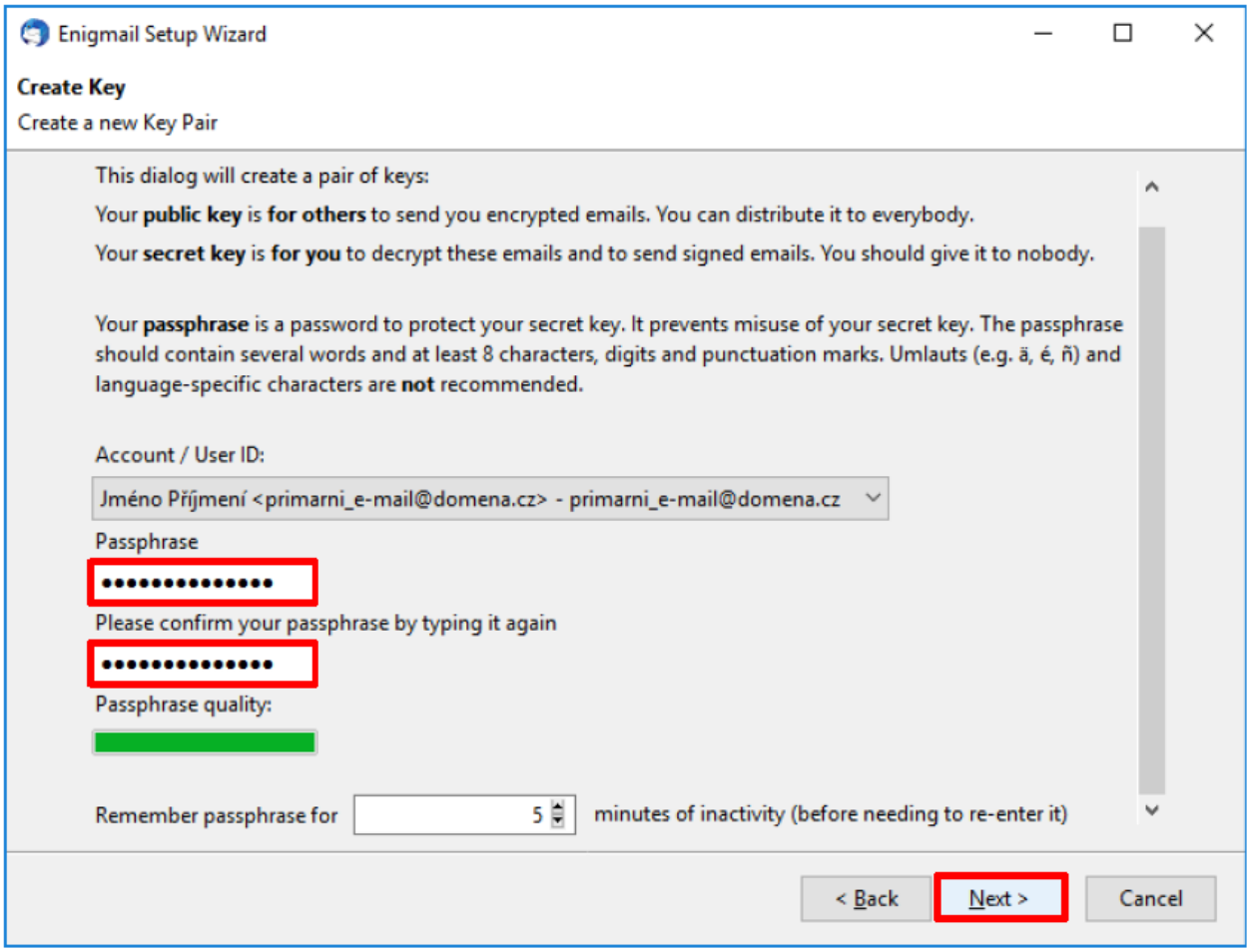
Nyní budete mít v dialogovém okně **možnost zvolit, zda chcete vytvořit nový pár klíčů**, v případě, že ještě žádný nemáte, nebo **naimportovat již existující** (v tom případě přeskočte, prosím, následující sekci na část Import PGP certifikátů).

Vytvoření vlastního PGP certifikátu

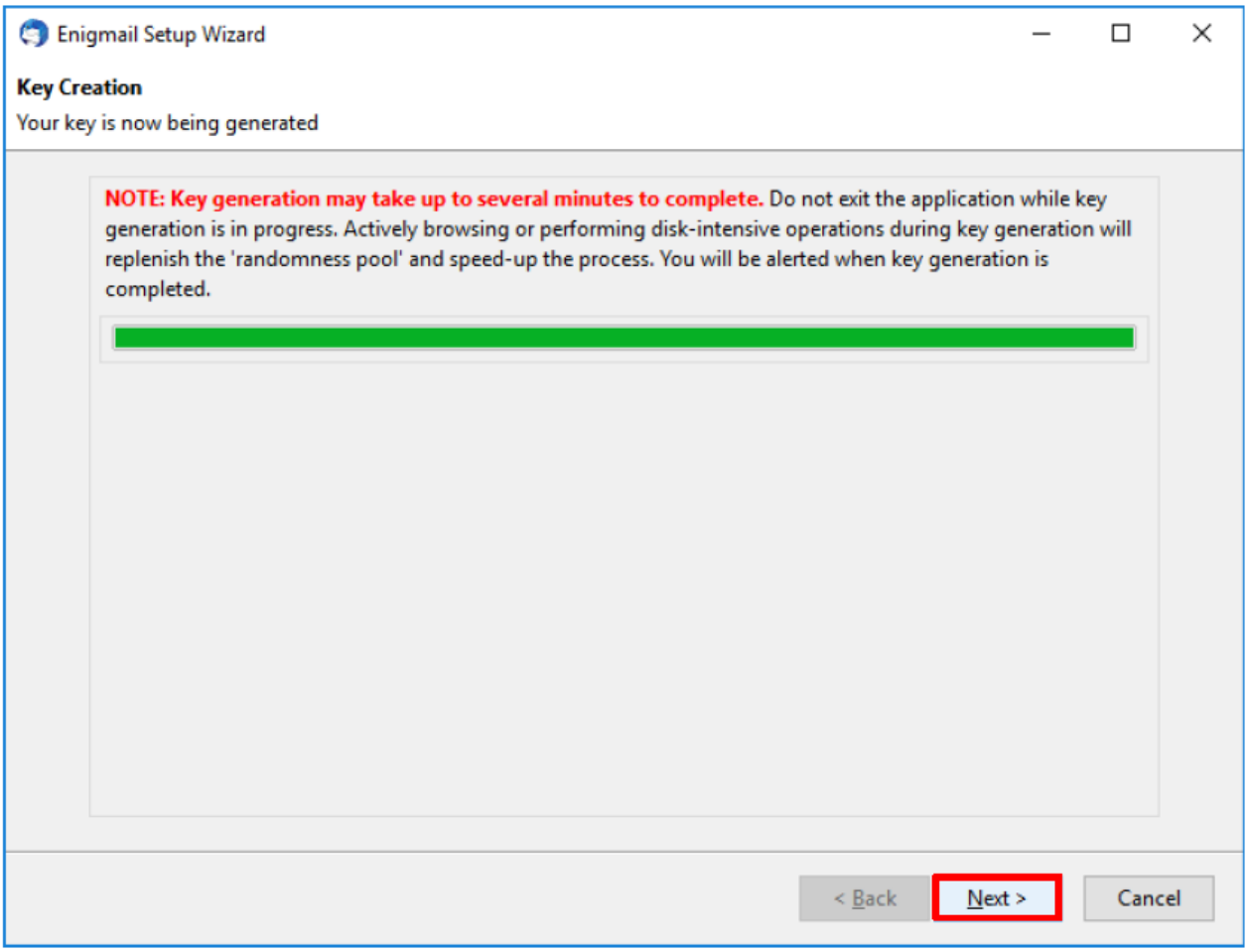
Pokud ještě **nemáte vlastní pár klíčů**, **zvolte** položku *„**I want to create a new key pair for signing and encrypting my email**"* *(Přeji si vytvořit nový pár klíčů pro podepisování a šifrování zpráv)* a **potvrďte** stiskem ***„Next"*.**



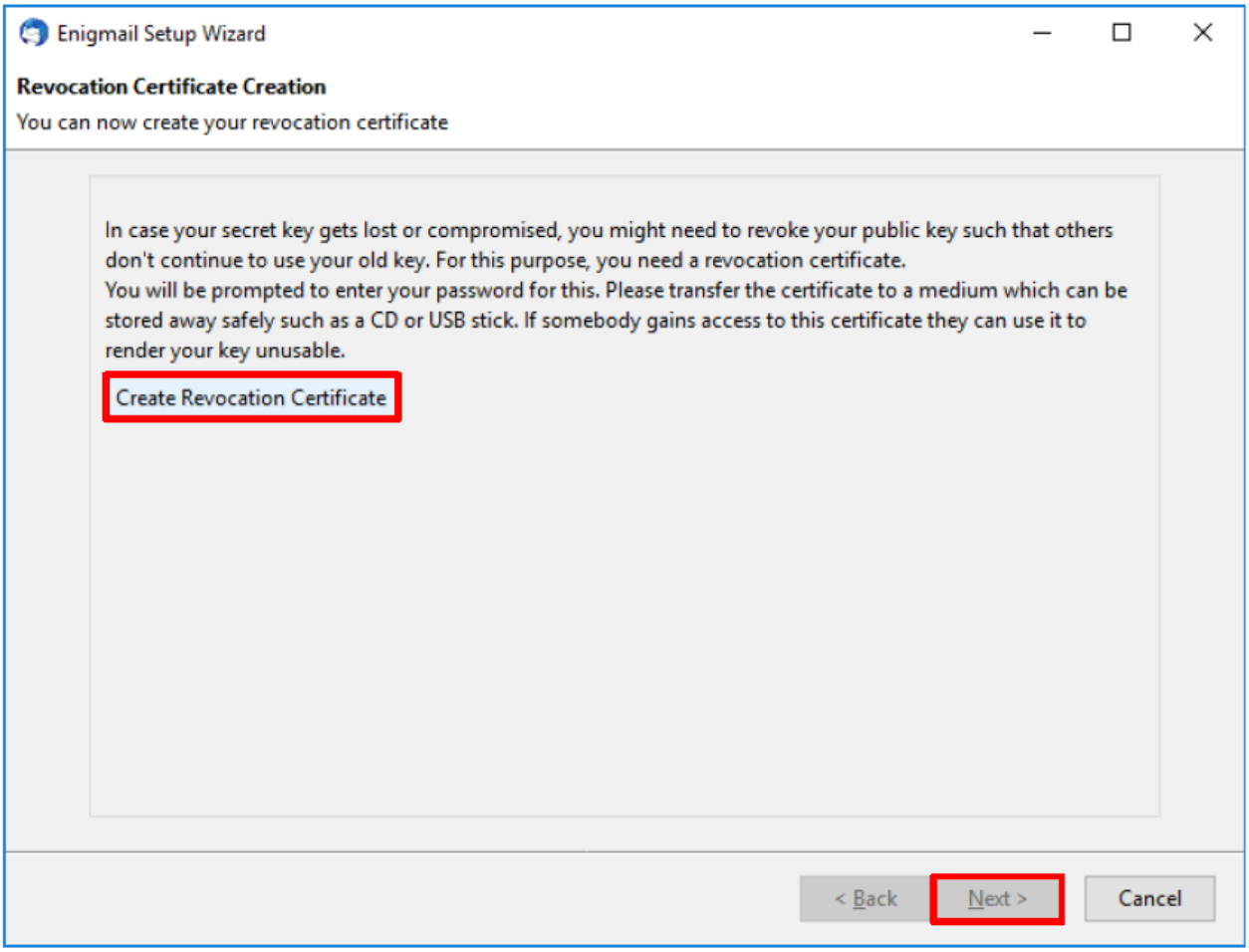
V dalším kroku musíte pro **vybraný pár klíčů zvolit heslo** do příslušných polí a **potvrdit** stiskem na ***„Další“*. Při tvorbě bezpečného hesla je vhodné aplikovat pravidla best-practices. Vygenerování silného a bezpečného hesla si můžete vyzkoušet zde.**



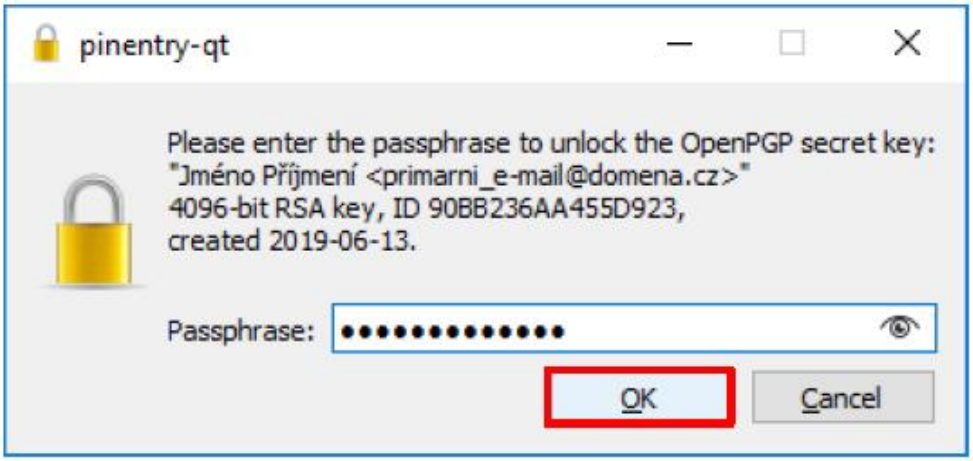
Rozběhne se proces generování klíčů, jehož rychlost (entropii) lze podpořit stisknutím libovolných kláves, či manipulací s jinými aplikacemi.



Posléze jste vyzváni, abyste vytvořili **revokační certifikát**, který **slouží k zneplatnění Vašeho klíče v případě, že dojde k jeho ztrátě či kompromitaci. Stiskněte *„Create Revocation Certificate*".**

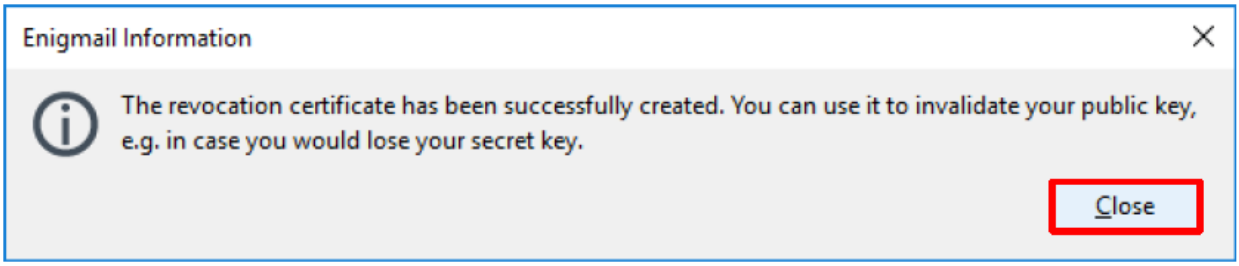


Dále jste vyzváni, abyste **zadali heslo**, které jste zvolili v předchozím kroku a vzápětí k **uložení revokačního certifikátu**.



V průběhu ukládání revokačního certifikátu **vyberte vhodnou lokaci**, kde jej v případě potřeby snadno dohledáte a **potvrďte** stiskem ***„Uložit"*.**

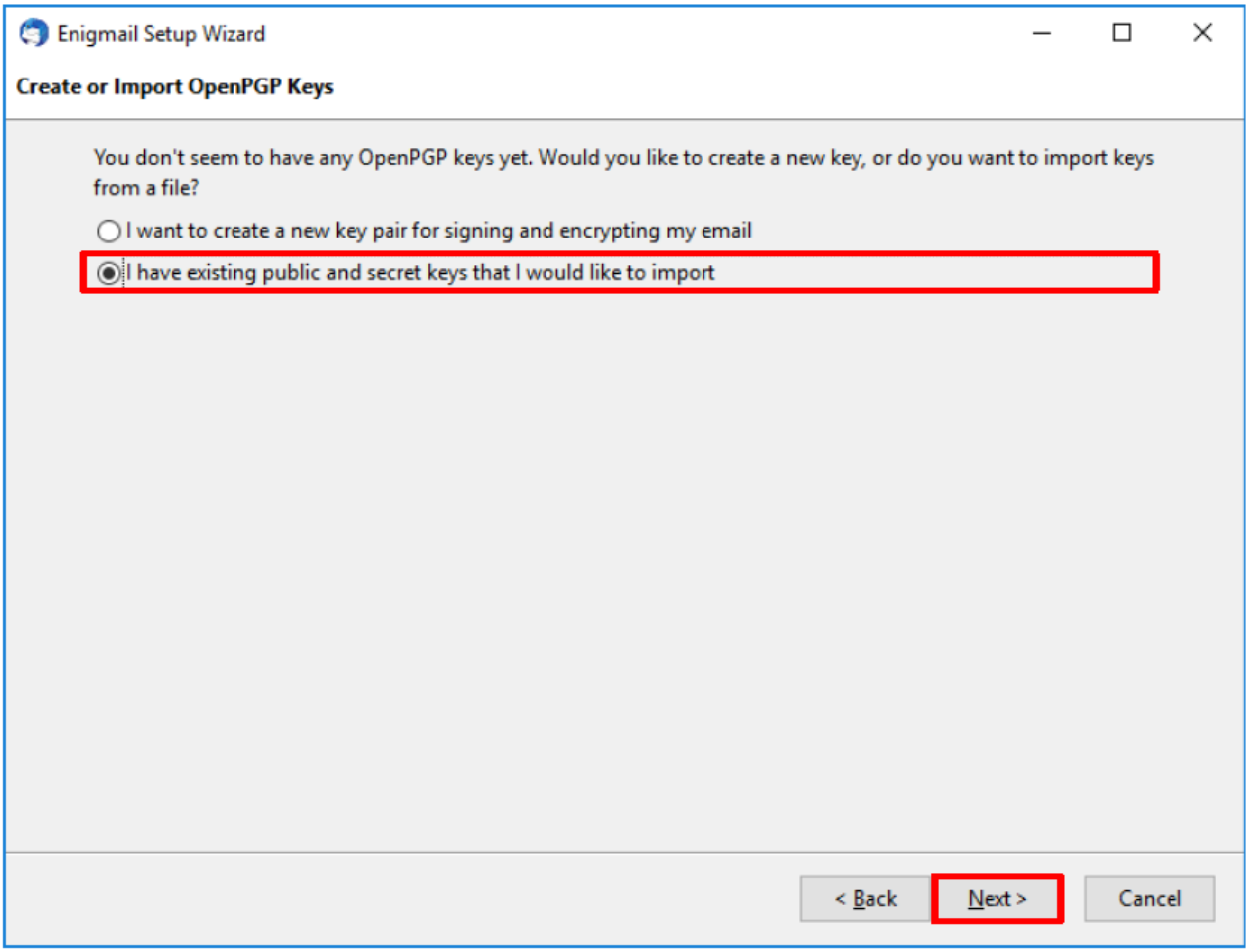
Následně se zobrazí **upozornění na bezpečné uložení revokačního certifikátu**, které je potřeba **potvrdit** stiskem na ***„OK"*.**



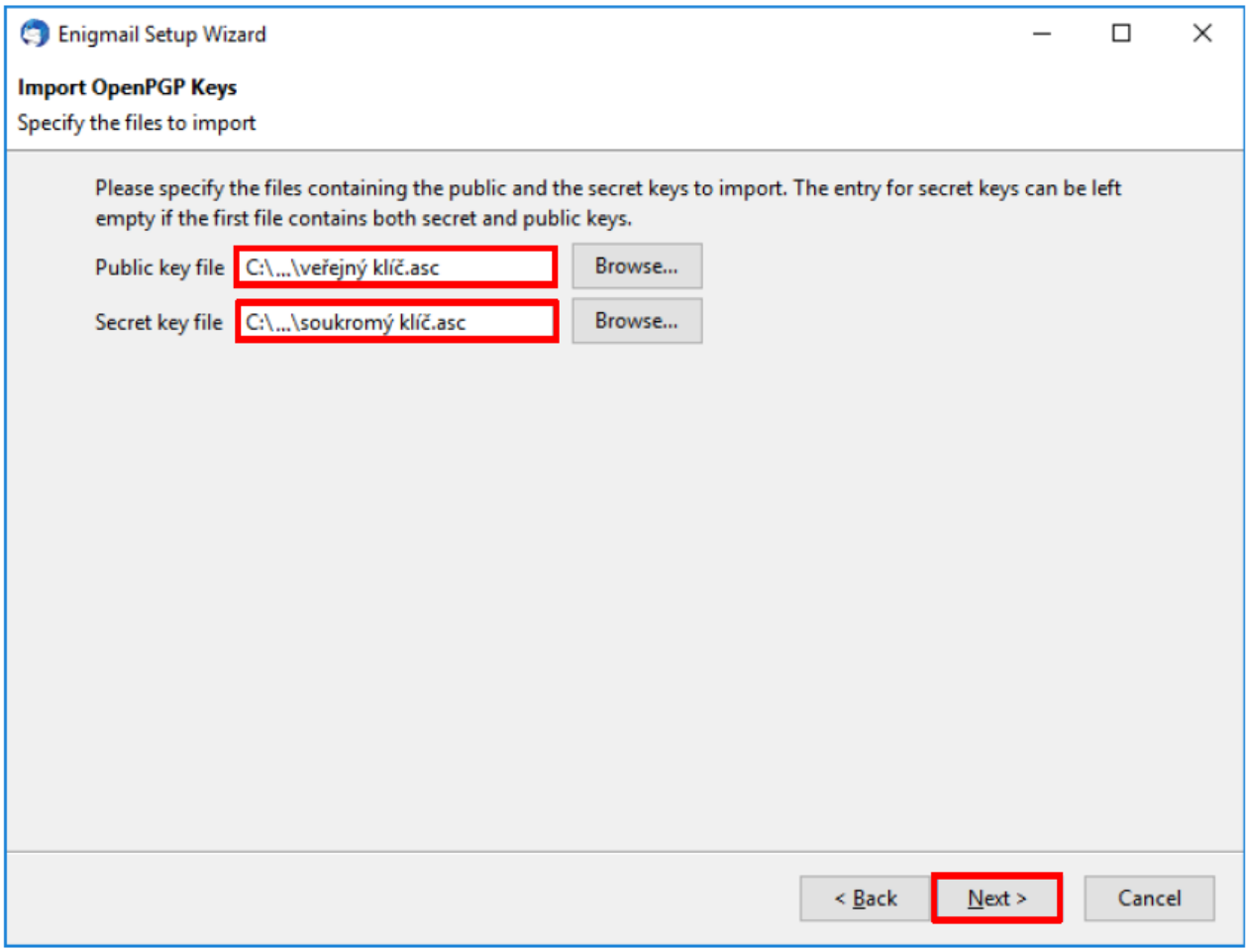
Po potvrzení upozornění pokračujte stisknutím ***„Next"*** *(Další)* v okně Průvodce nastavením Enigmail a **potvrďte jeho dokončení**.

Import vlastního PGP certifikátu

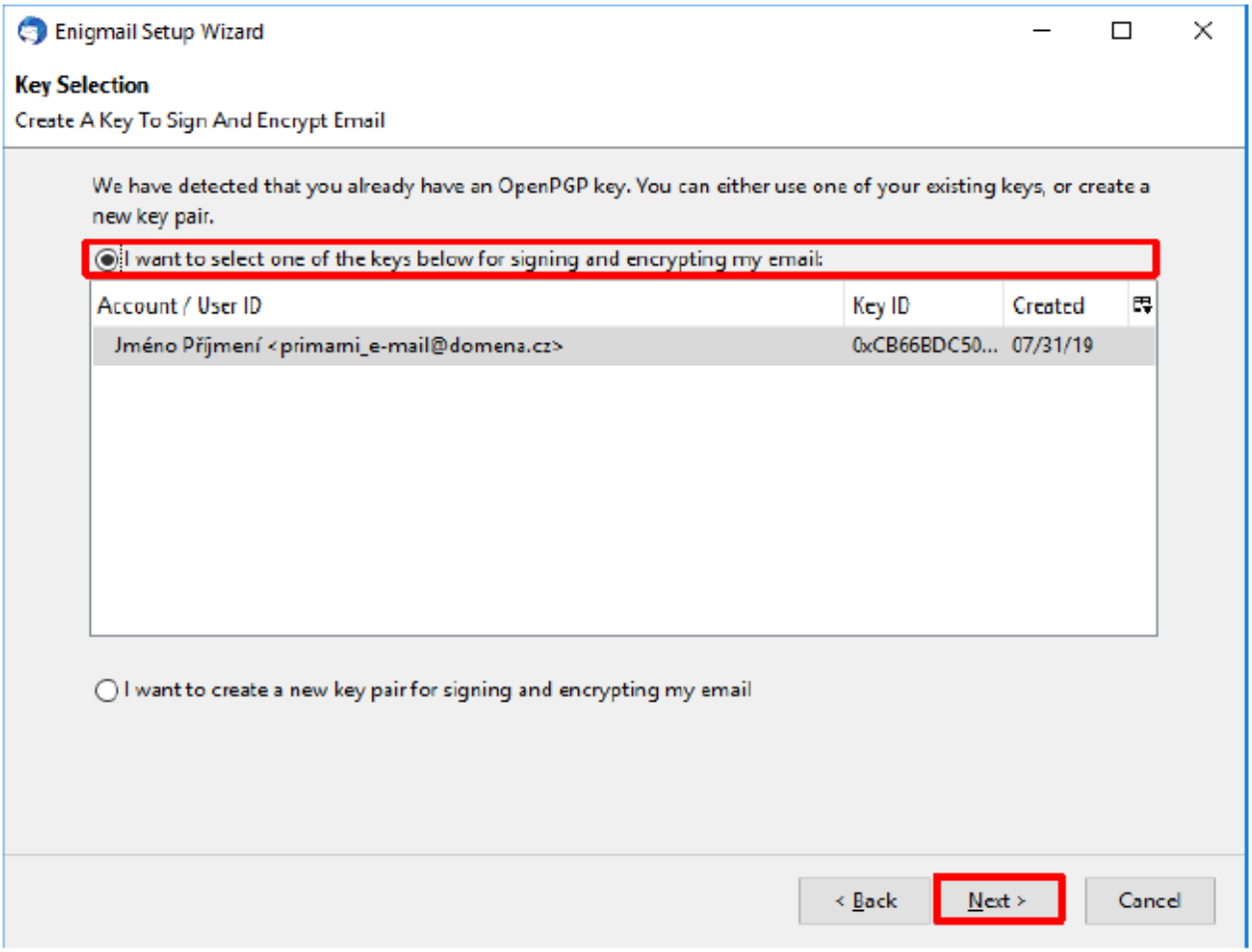
Pokud již **vlastníte svůj pár klíčů**, můžete jej do Enigmail **naimportovat**. V Průvodci nastavením Enigmail **zvolte** druhou **možnost *„I have existing public and secret keys that I would like to import"*** (*Mám vytvořený pár veřejného a soukromého klíče a chci jej importovat)*. Potvrďte ***„Next"*** *(Další).*



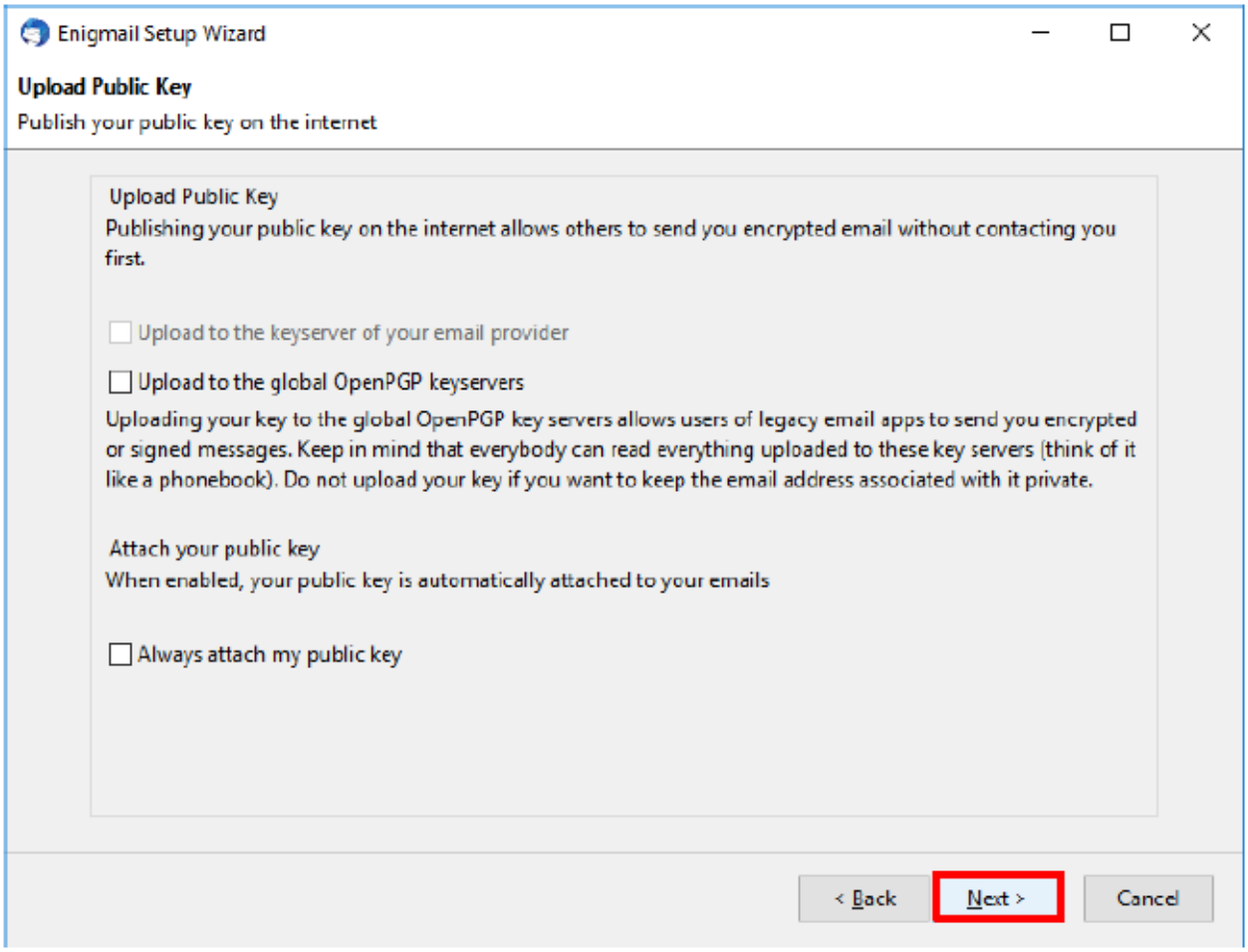
Nyní je třeba do příslušných polí **zadat cestu k Vašemu veřejnému a soukromému klíči.** Potvrďte ***„Next"*** (*Další)*.



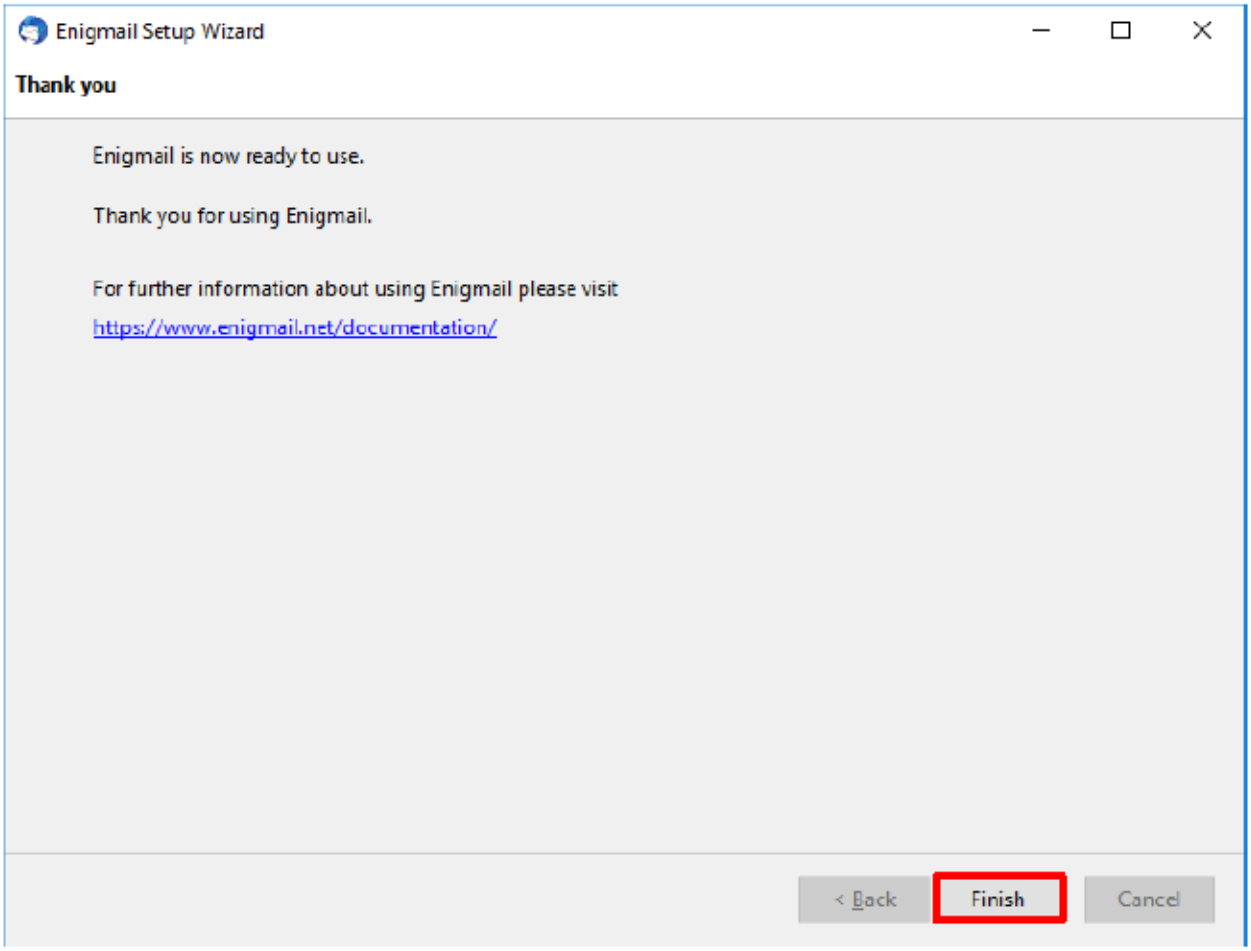
V dalším kroku je třeba **označit položku *„I want to select one of the keys below for signing and encrypting my emails"*** *(Přeji si vybrat jeden z níže uvedených klíčů pro podepisování a šifrování svých zpráv)* a vybrat Váš **importovaný klíč**. **Potvrďte *„Next".***



Dále máte **možnost zvolit**, zda bude Váš **veřejný klíč nahrán na jeden z globálních serverů**. Pokud si nejste jisti, nebo **pokud nechcete sdílet** svůj veřejný klíč úplně všem uživatelům internetu, neoznačujte žádnou možnost. Tuto volbu můžete uskutečnit kdykoliv později.

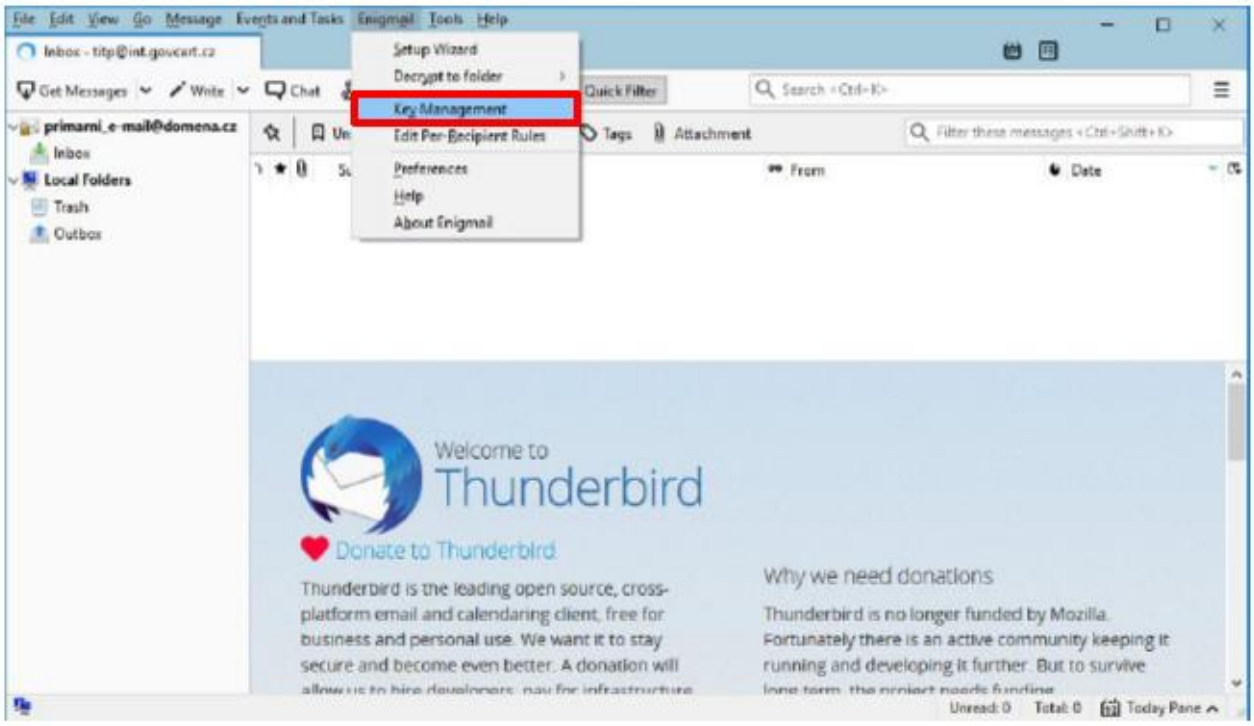


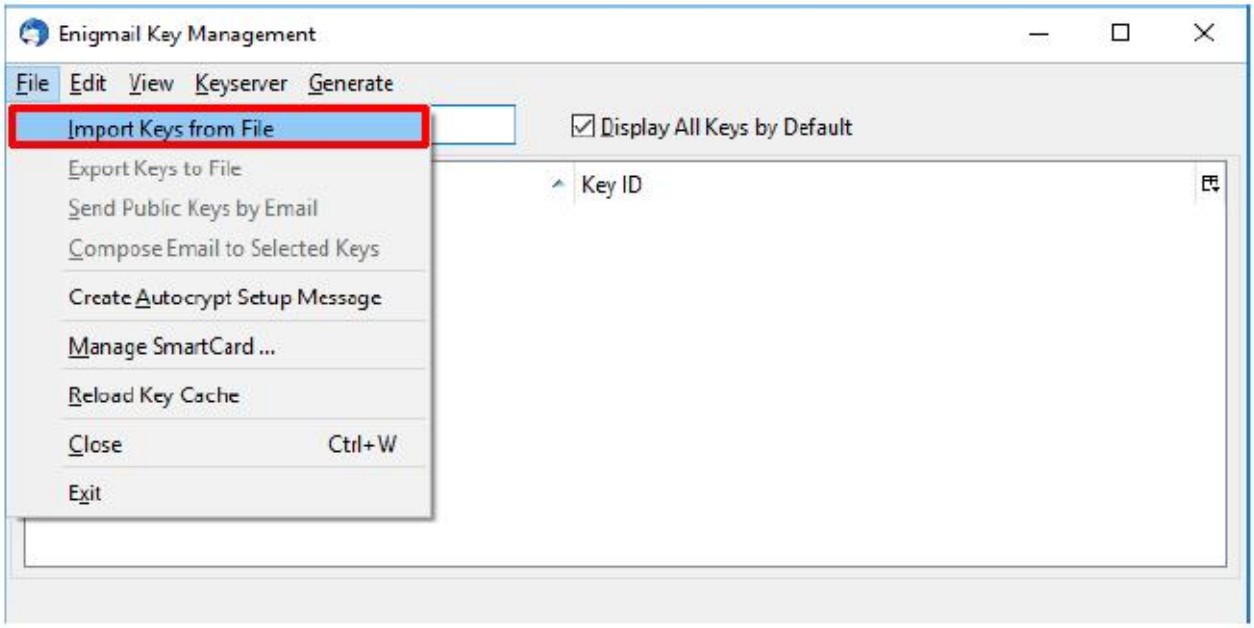
Následně **dokončíme nastavení.**



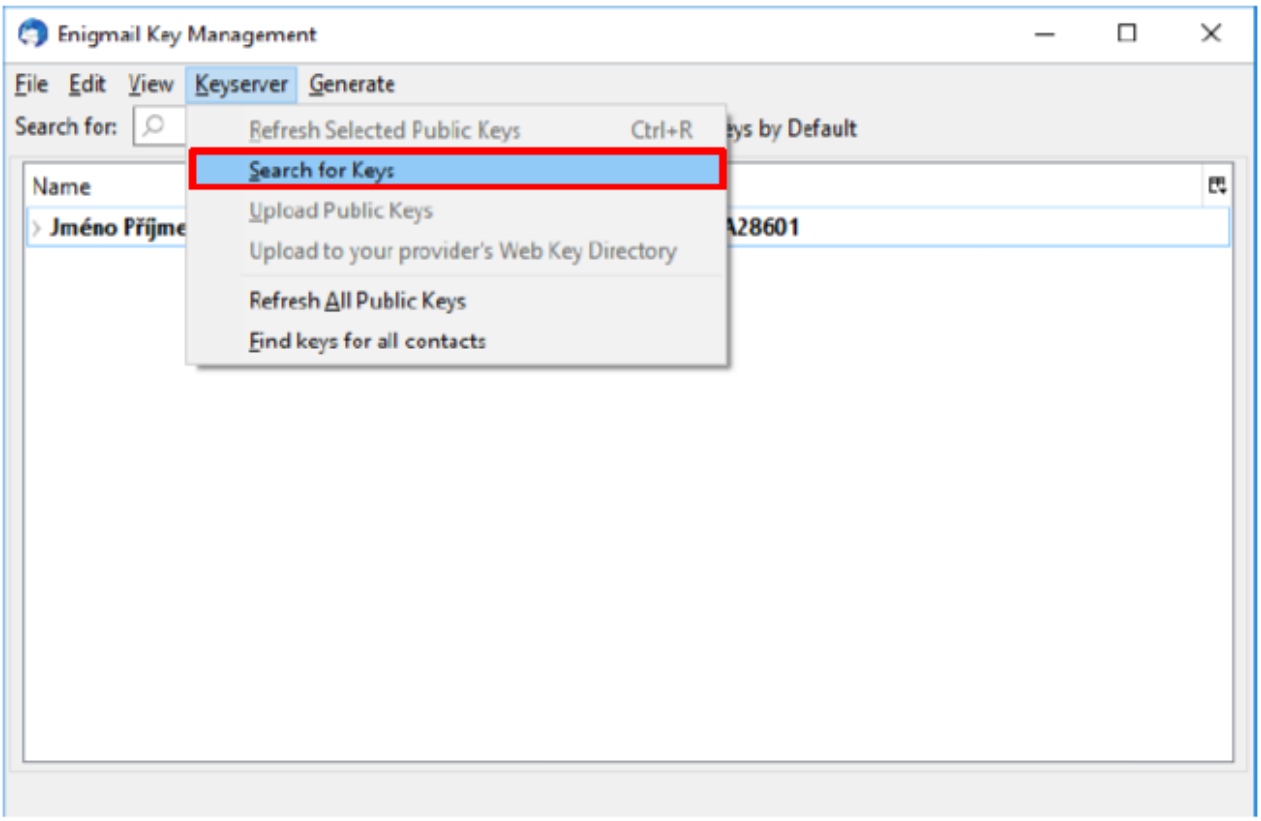
Import PGP certifikátů příjemců

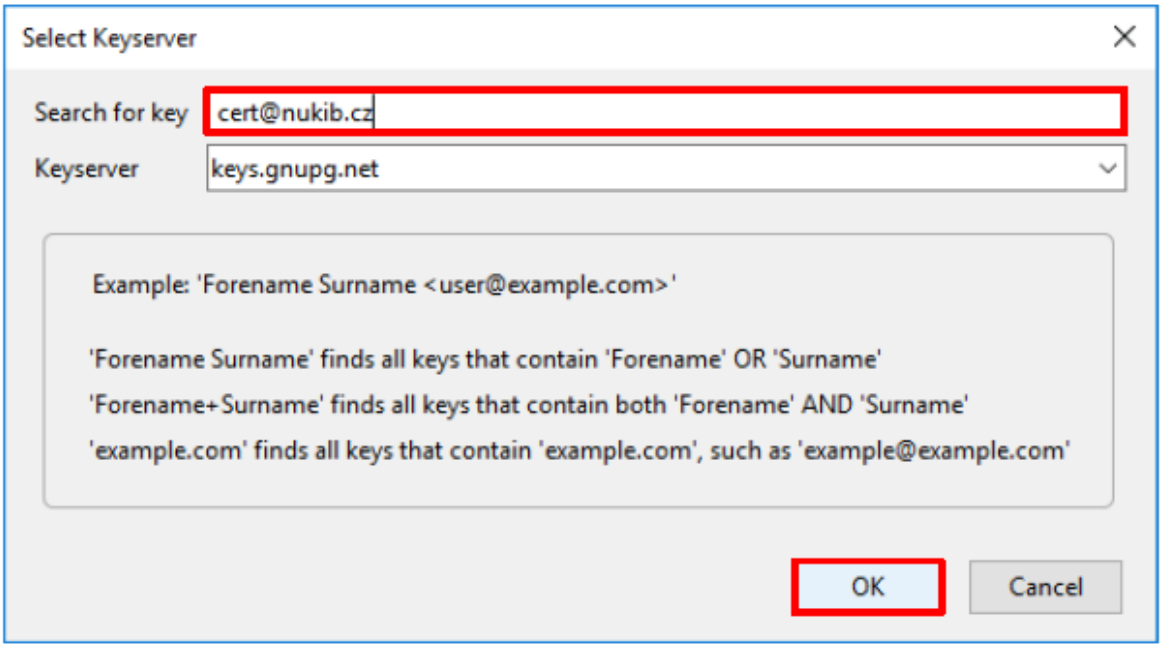
Nyní zbývá **naimportovat PGP klíče příjemců**, což provedete následovně: ***„Enigmail" -> „Key management"*** *(Správa klíčů).* Pokud Vám byly veřejné klíče zaslány e-mailem, nebo jste je stáhli z důvěryhodného zdroje, pokračujte: ***„File" -> „Import Keys from File"*** *(Soubor -> Importovat klíče ze souboru).*



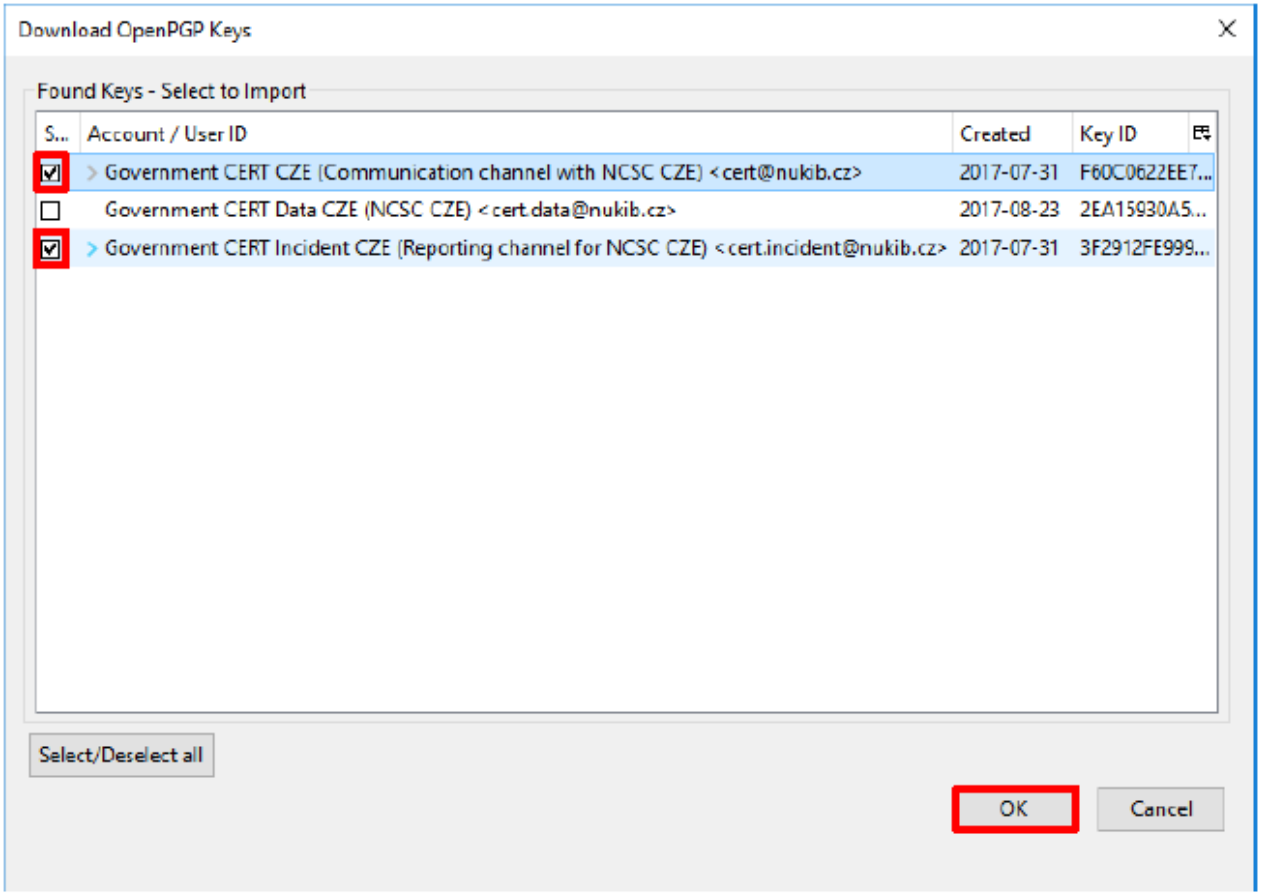


V případě, že **znáte jméno vlastníka či organizace**, se kterými chcete šifrovaně komunikovat, lze jejich **veřejný klíč dohledat i na některém z keyserverů.** Ve ***„Key Management"* -> *„Keyserver"* -> *„Search for Keys"*** *(Správa klíčů -> Keyserver -> Hledat klíče)* zadejte do příslušné kolonky hledaný výraz (např. název organizace), vyberte vhodný keyserver a **potvrďte „OK".**

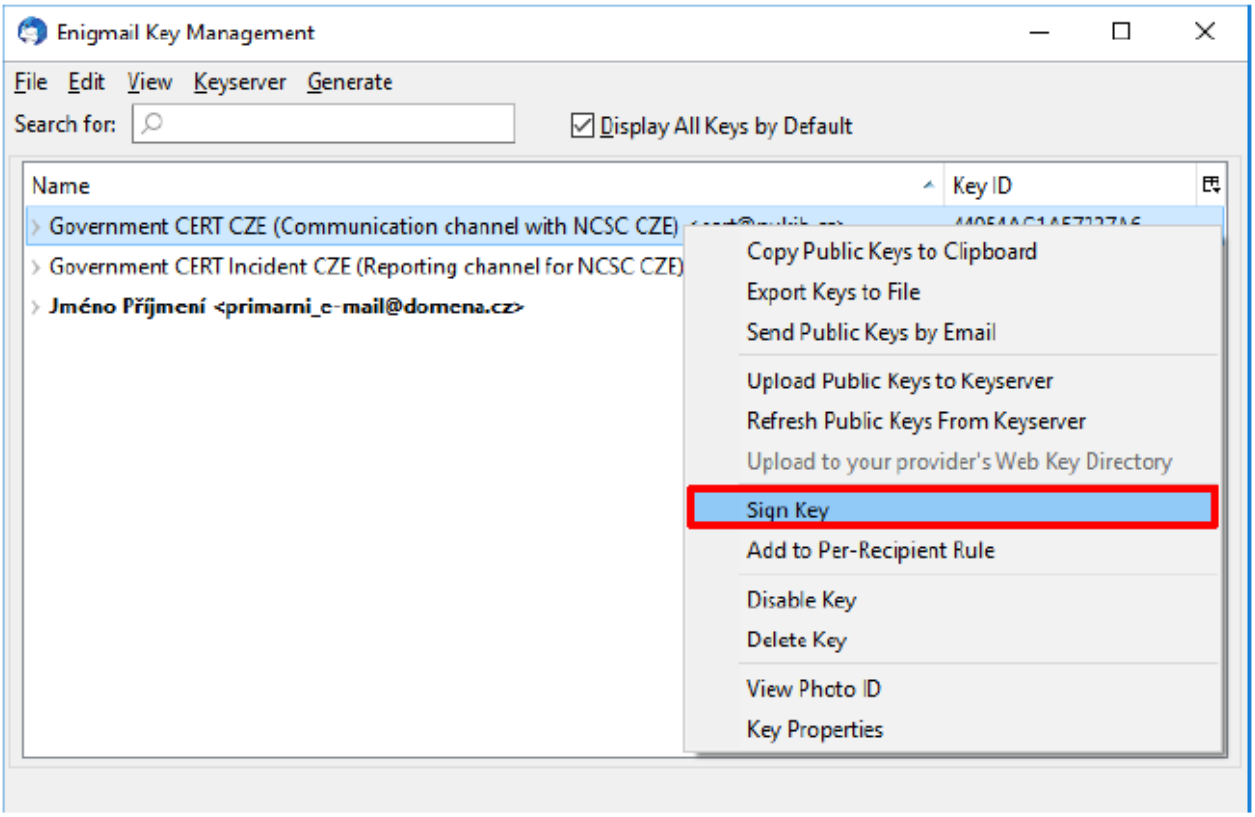




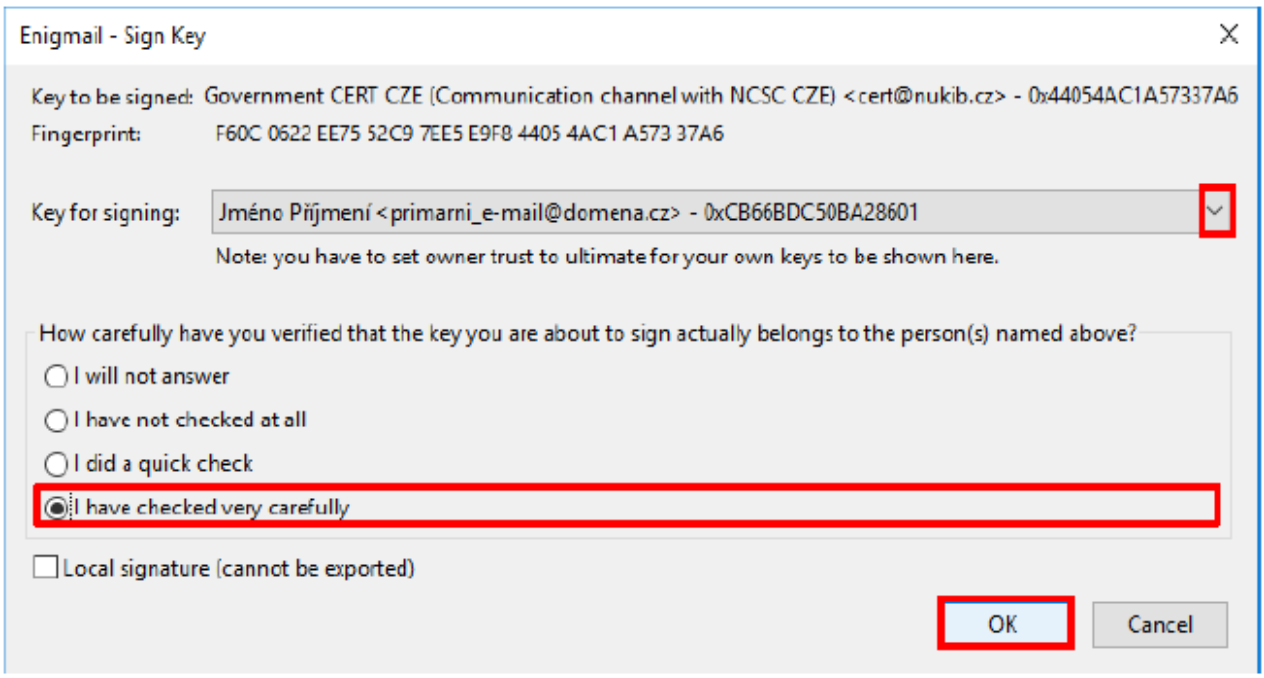
Posléze **označte požadované veřejné klíče**, které ze serveru **stáhnete.**



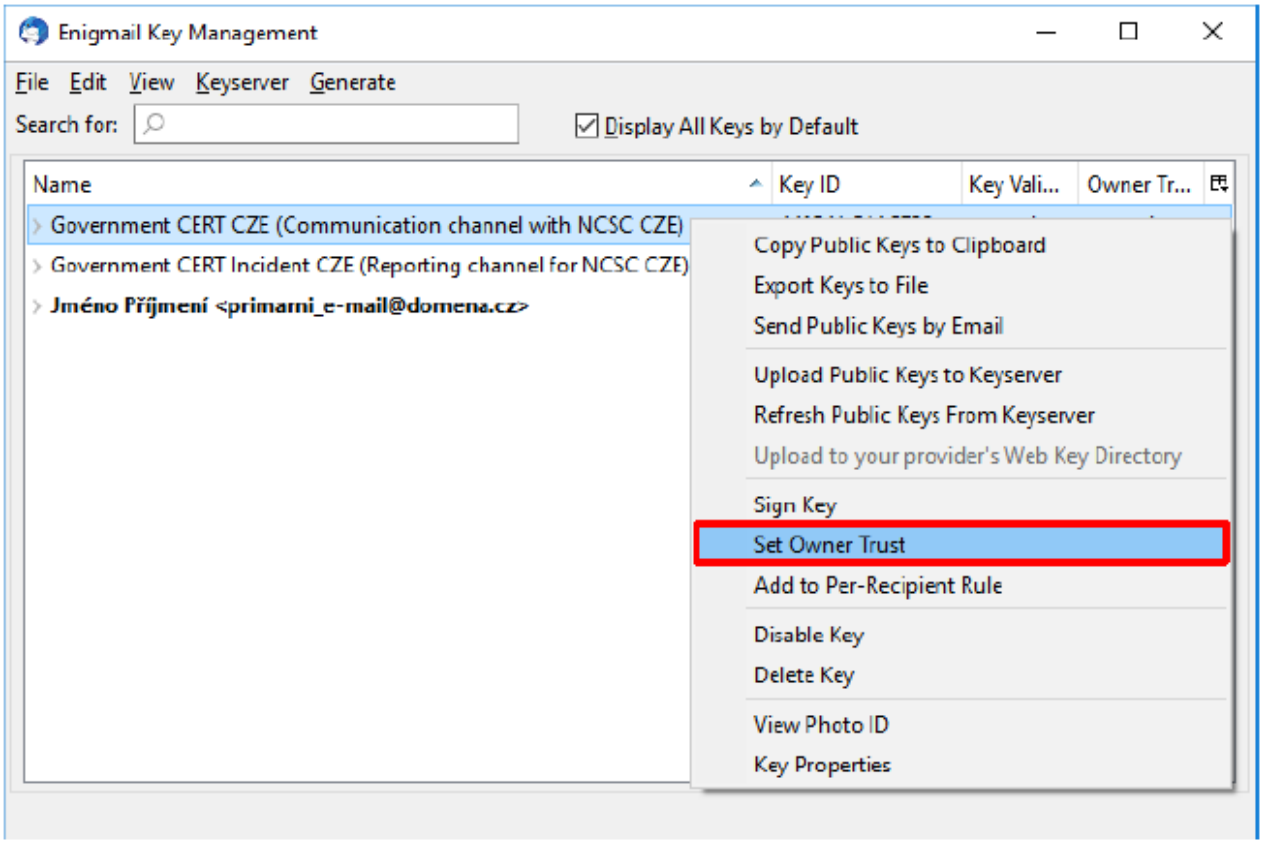
Po **naimportování potřebných klíčů** příjemců je potřeba tyto **klíče nejprve podepsat** a **nastavit jejich důvěryhodnost**. To se provede takto: pravým tlačítkem myši **vyberte příslušný PGP klíč** a zvolte možnost ***„Sign Key"*** *(Podepsat klíč).*



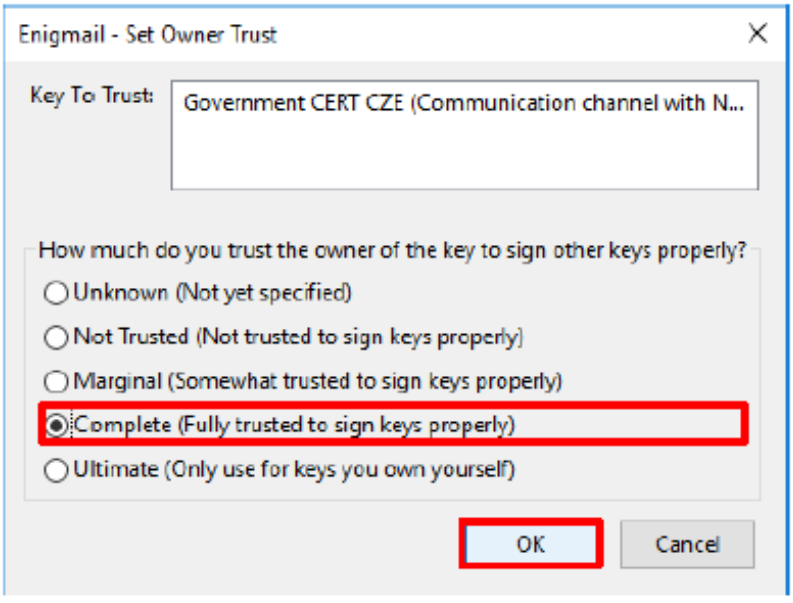
Vyberte svůj vlastní klíč**, kterým budete vybraný klíč příjemce podepisovat a** zvolte míru Vašeho ověření**, že daný klíč patří vlastníku – v tomto případě bezpečnostnímu týmu CSIRT SŽ.**



Dále opět **pravým tlačítkem myši vyberte příslušný klíč** a **zvolte** možnost ***„Set Owner Trust"*** *(Nastavit důvěryhodnost vlastníka)*. Tato **možnost je aktivní teprve až po podpisu klíče** (viz předchozí krok).

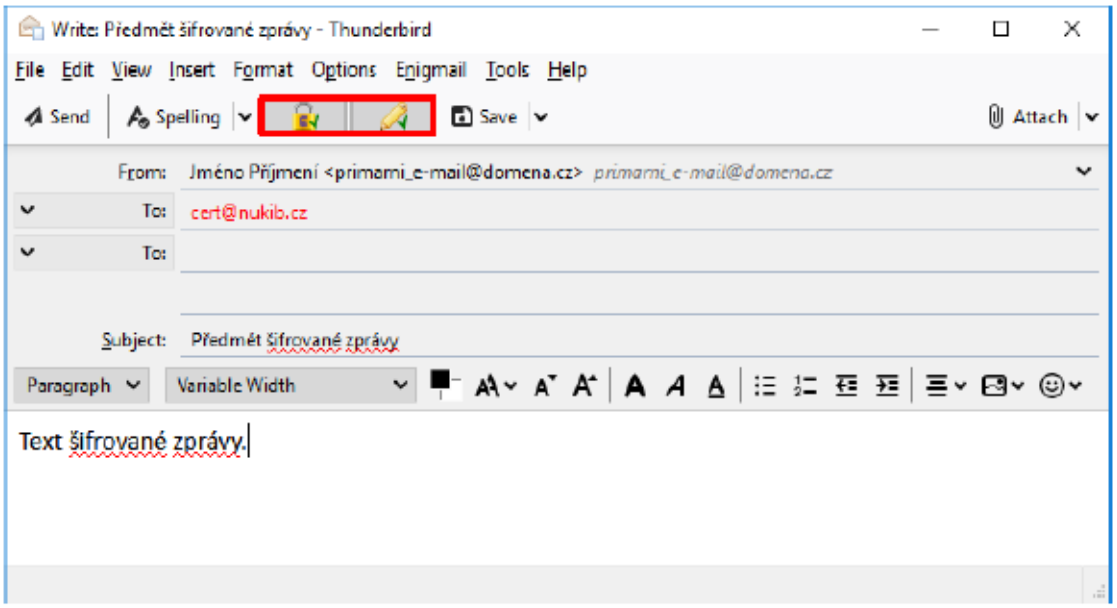


Hodnotu u klíče příjemce nastavíte **dle jeho důvěryhodnosti**. V případě klíče bezpečnostního týmu CSIRT SŽ například **nastavte *„Complete"*** *(Plně důvěřuji)*, pokud protější straně důvěřujete. V případě **vlastního klíče** (odesílatele) **nastavte** na ***„Ultimate"*** *(Absolutně důvěřuji)*. **Nyní již lze odesílat a přijímat šifrované zprávy.**

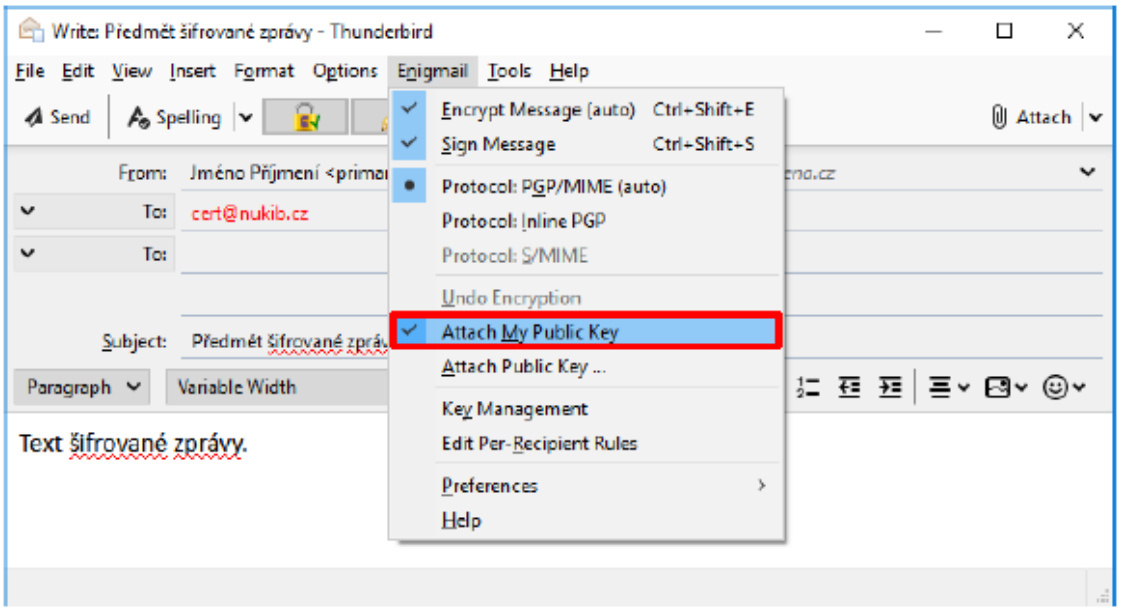


Šifrování e-mailové zprávy

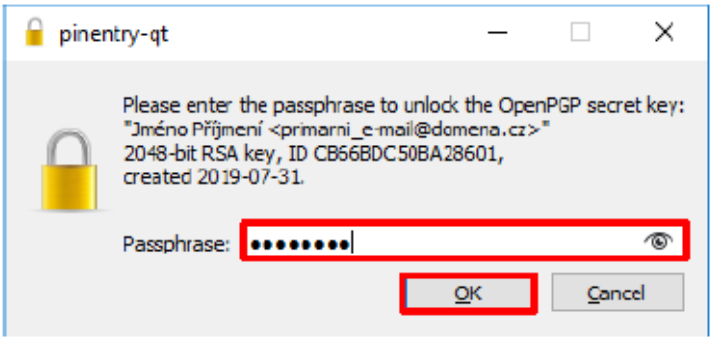
Způsob **šifrování e-mailu** v aplikaci **Mozilla Thunderbird** je následující: v hlavním menu zvolte možnost ***„Write"*** *(Napsat)* a po otevření okna s novou zprávou **vyplňte standardní údaje** (e-mailovou adresu příjemce, předmět a tělo zprávy). E-mail **následně zašifrujete** kliknutím na ikonu ***„zámku"*** a pokud chcete zprávu **podepsat,** klikněte na ikonku ***„tužky".***



Pro **obousměrnou šifrovanou komunikaci označte** v řádku „Enigmail" a vyberte položku ***„Attach My Public Key"*** (*Připojit můj vlastní veřejný klíč).*



Následně **budete vyzváni k zadání hesla** a **po jeho potvrzení již dojde k odeslání šifrované zprávy.**



Nastane-li situace, že **zadané e-mailové adrese příjemce neodpovídá žádný z uložených veřejných klíčů**, je **odesílatel před odesláním zprávy vyzván k výběru odpovídajícího klíče.**

Nyní by již nic nemělo bránit v šifrované komunikaci mezi Vámi a Vašimi partnery.