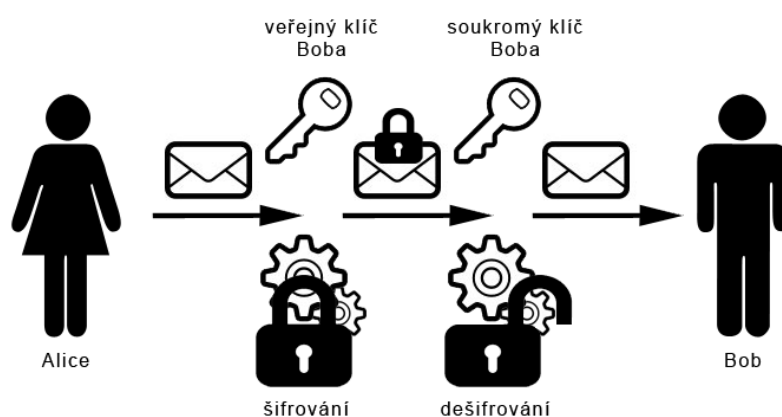


## Šifrování e-mailových zpráv pomocí PGP v aplikacích MS Outlook a Mozilla Thunderbird

Tento dokument představuje jednoduchý návod pro realizaci šifrované e-mailové komunikace s týmem vládního CERTu (dále jen GovCERT.CZ). Prezentuje šifrování, dešifrování a podepisování e-mailových zpráv pomocí PGP klíčového páru s využitím dvou nejpoužívanějších aplikací **MS Outlook** (str. 2) a **Mozilla Thunderbird** (str. 16).

Pro šifrování, dešifrování a digitální podepisování e-mailových zpráv využívá tým GovCERT.CZ 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). Současně slouží soukromý klíč 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 GovCERT.CZ jsou umístěny veřejné klíče, které jsou určeny pro komunikaci s naším týmem. První z nich je využíván pro běžnou komunikaci na e-mailovou adresu [cert@nukib.cz](mailto:cert@nukib.cz). Druhý veřejný klíč slouží pro hlášení incidentů na e-mailovou adresu [cert.incident@nukib.cz](mailto:cert.incident@nukib.cz).

## 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):

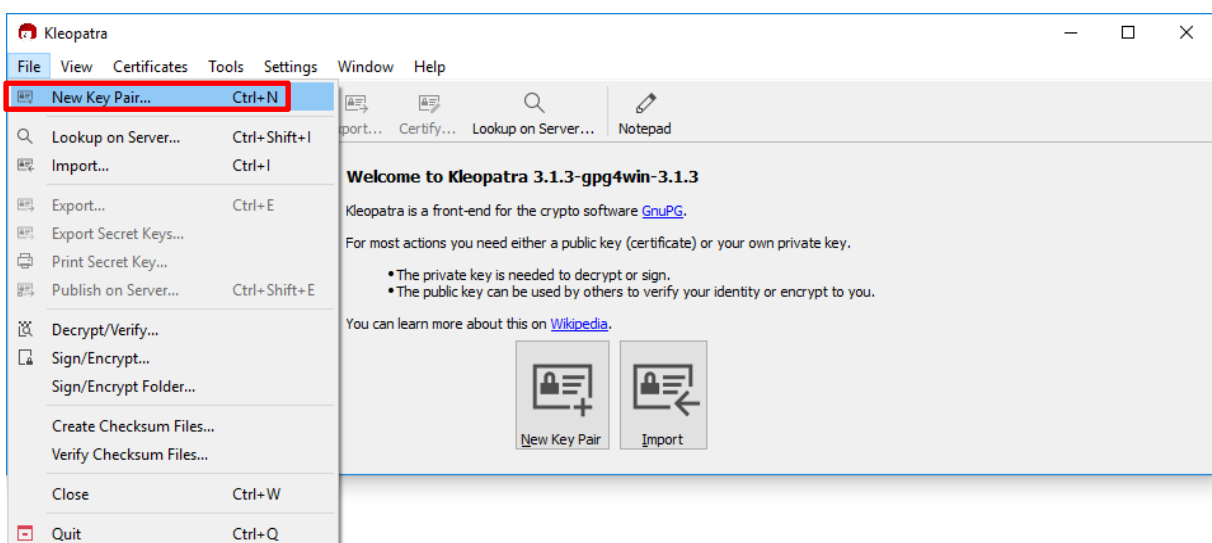
- **GnuPG – šifrovací nástroj**
- **Kleopatra – správce klíčů pro OpenPGP a X.509 (S/MIME)**
- GPA – alternativní správce klíčů
- GpgEX – plugin pro Microsoft Explorer
- **GpgOL – plugin pro MS Outlook 2010/2013/2016 (32 i 64 bit verze)**
- Compendium – dokumentace v angličtině a němčině

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.

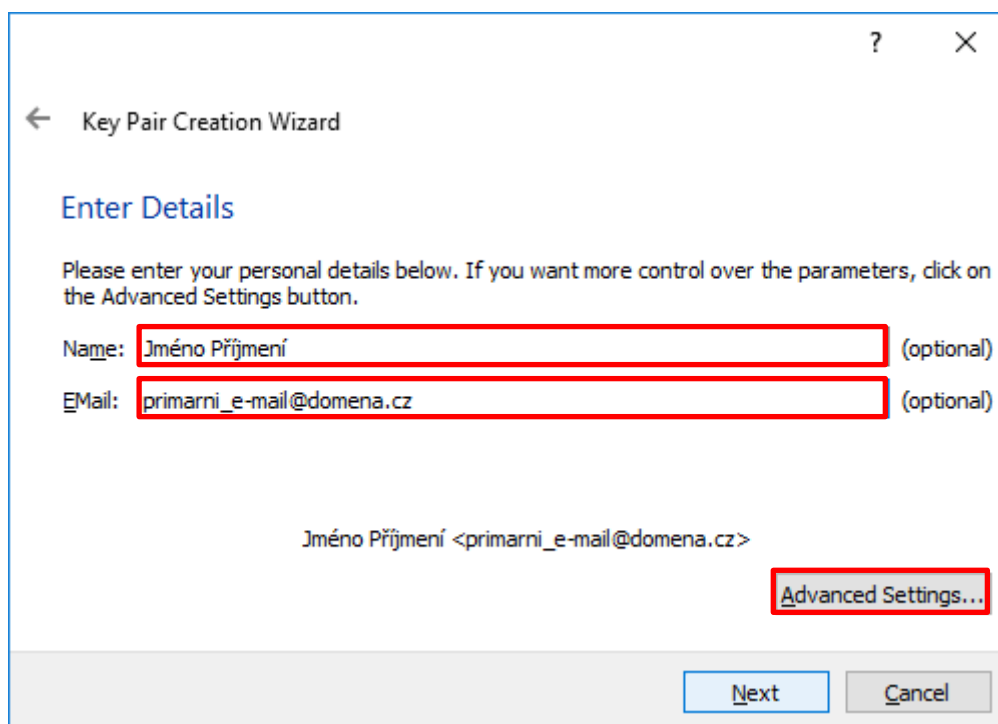
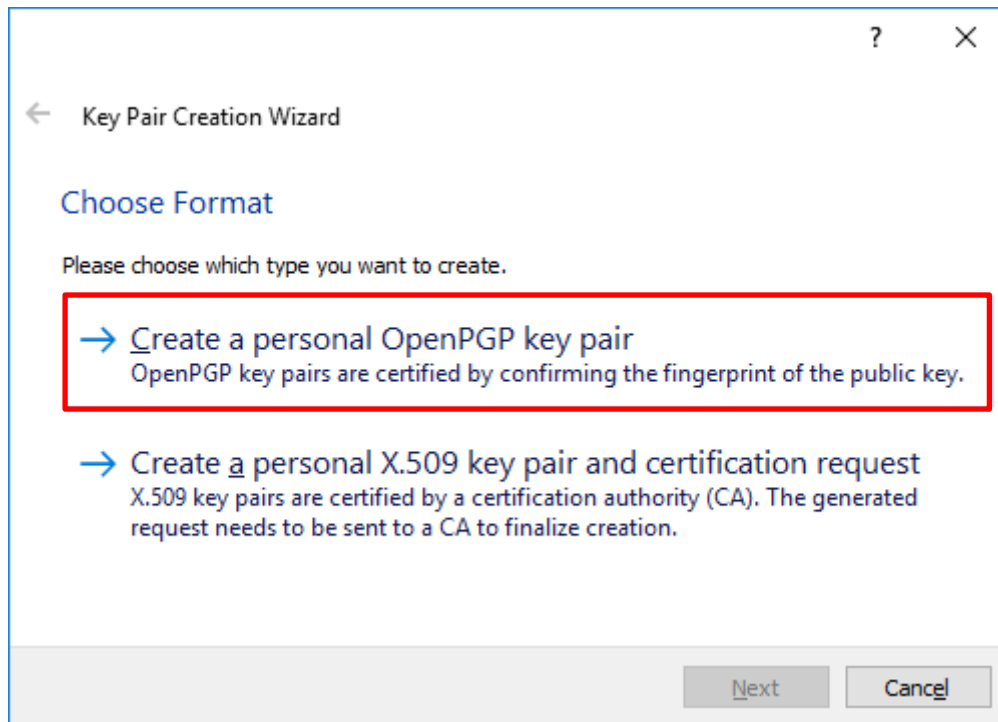
Po nainstalování potřebných pluginů a aplikací z balíčku GPG4Win spusťte aplikaci **Kleopatra**. V případě, že již máte svůj PGP klíč, můžete následující krok „Vytvoření vlastního PGP certifikátu“ přeskočit.

## Vytvoření vlastního PGP certifikátu v aplikaci Kleopatra

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

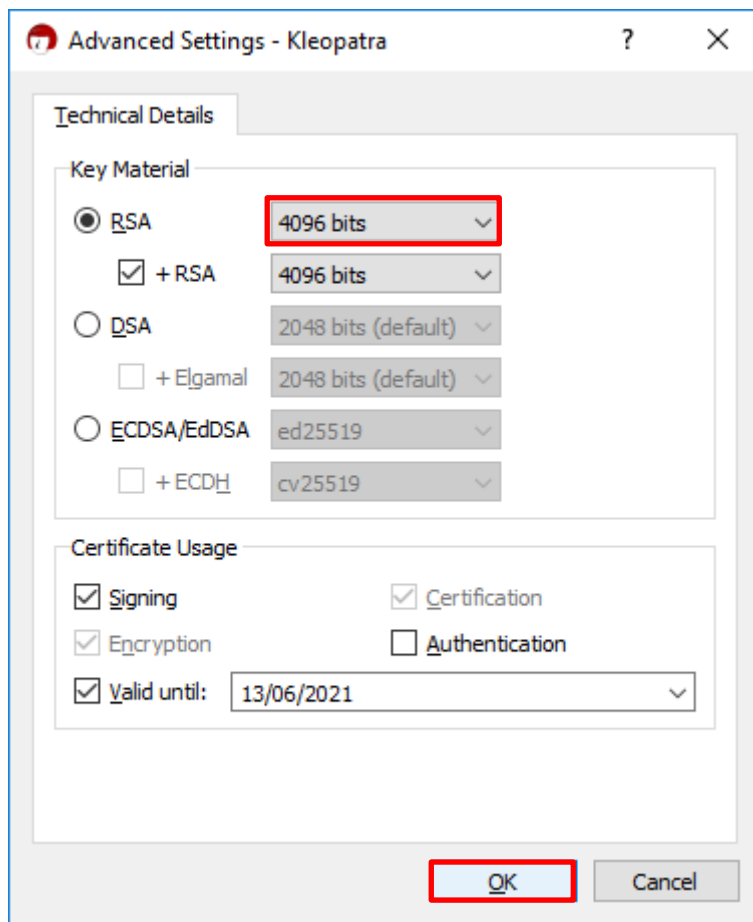


Následně zvolte „*Create a personal OpenPGP key pair*“ a v dalším okně vyplňte odpovídající údaje.

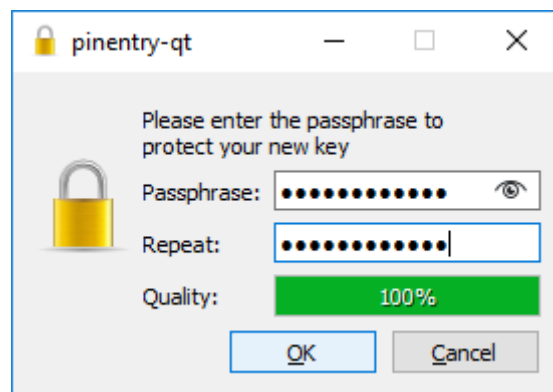
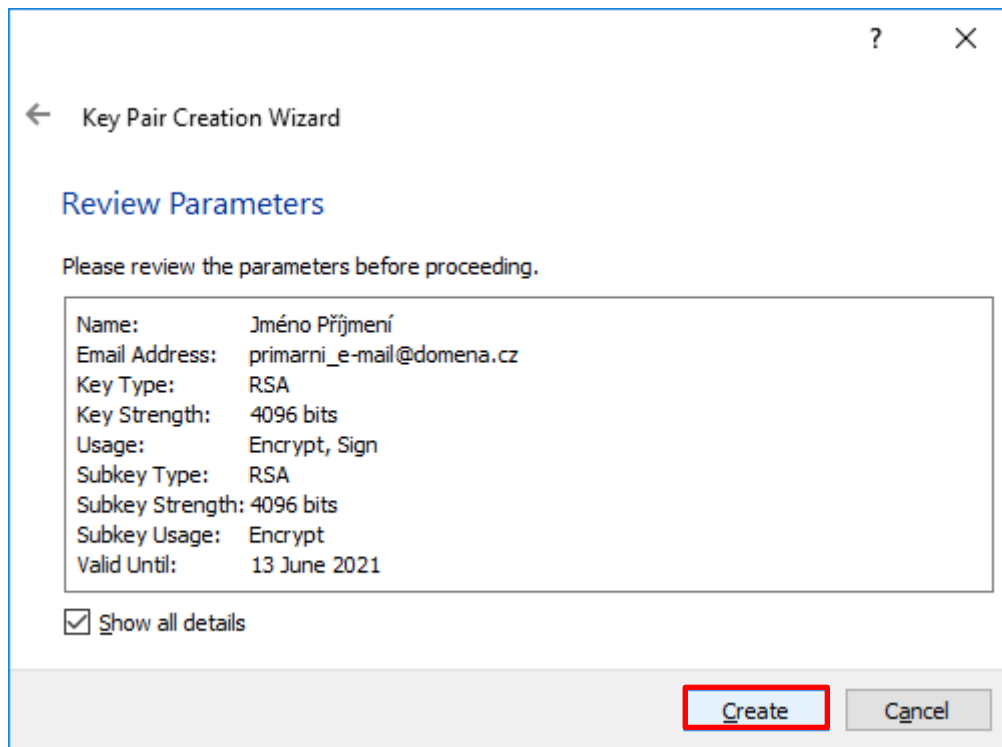


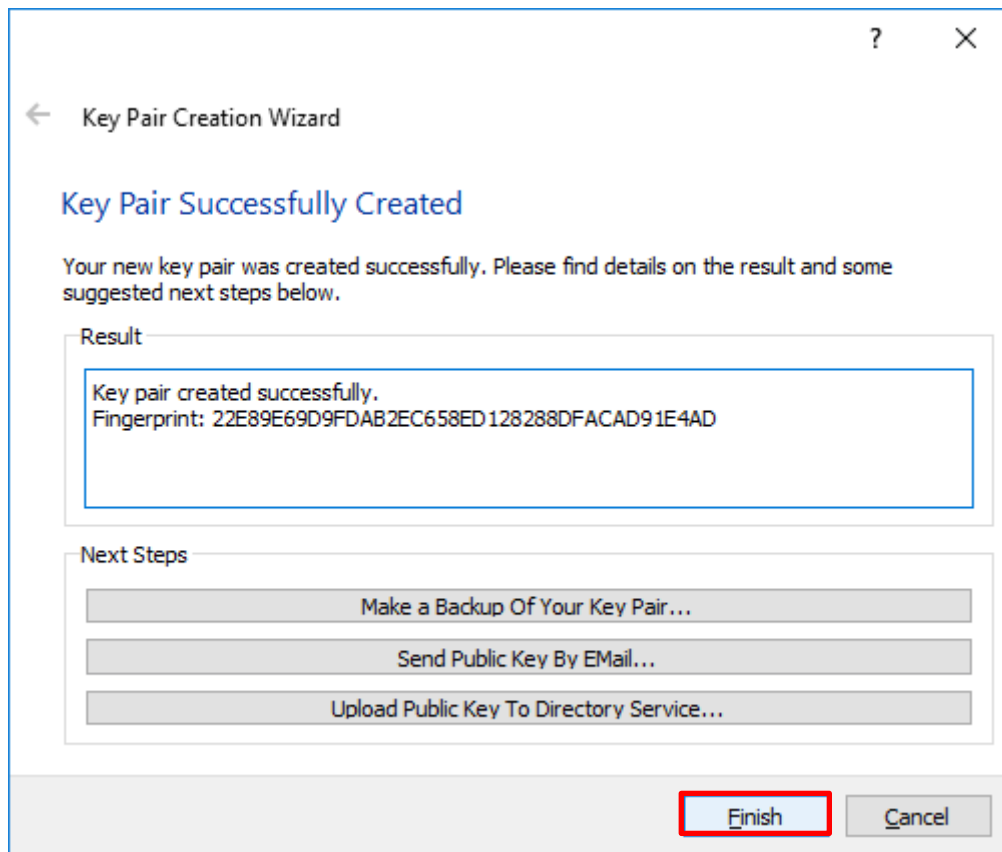
Posléze stiskněte tlačítko „*Advanced Settings...*“.

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

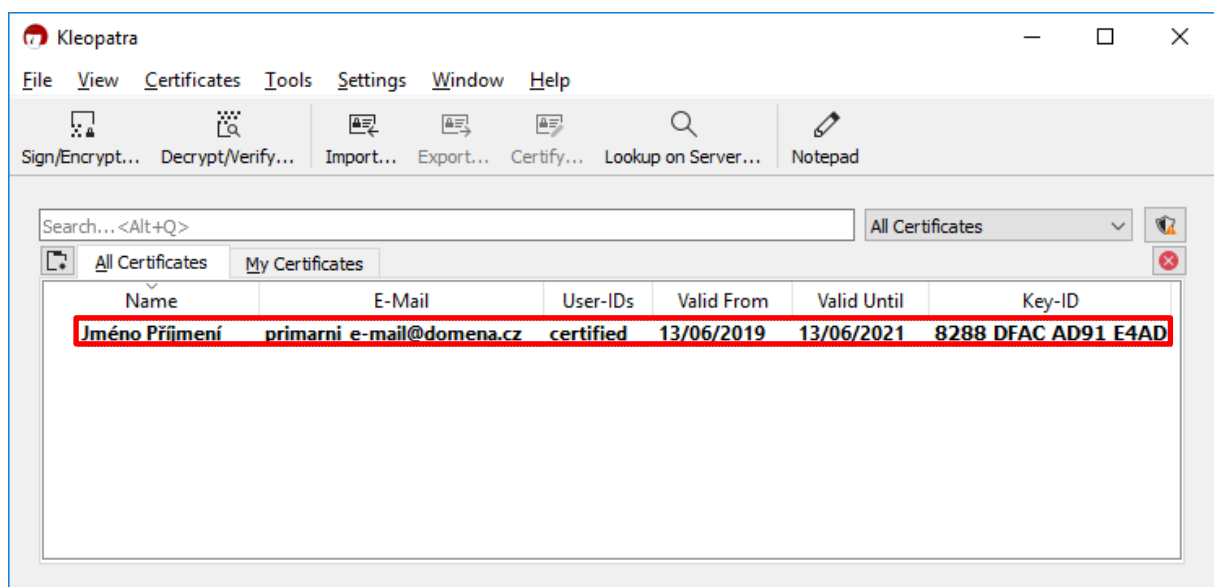


Zkontrolujte zadané parametry a stiskem „Create“ začne aplikace generovat samotné klíče. V průběhu budete vyzváni k zadání a potvrzení hesla, které slouží jako autentizace vlastníka certifikátu, čímž se chráníte před jeho případným odcizením. Při tvorbě bezpečného hesla je vhodné aplikovat pravidla [best-practise](#).





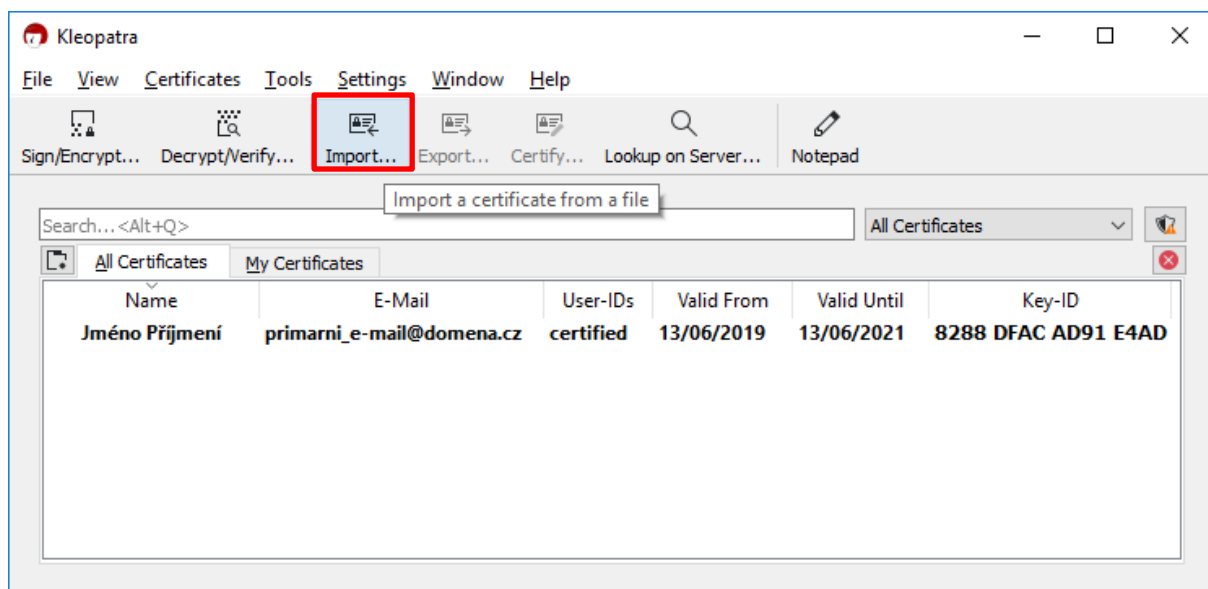
Po dokončení procesu generování páru klíčů máte několik možností jak je uložit a stiskněte tlačítko „Finish“.



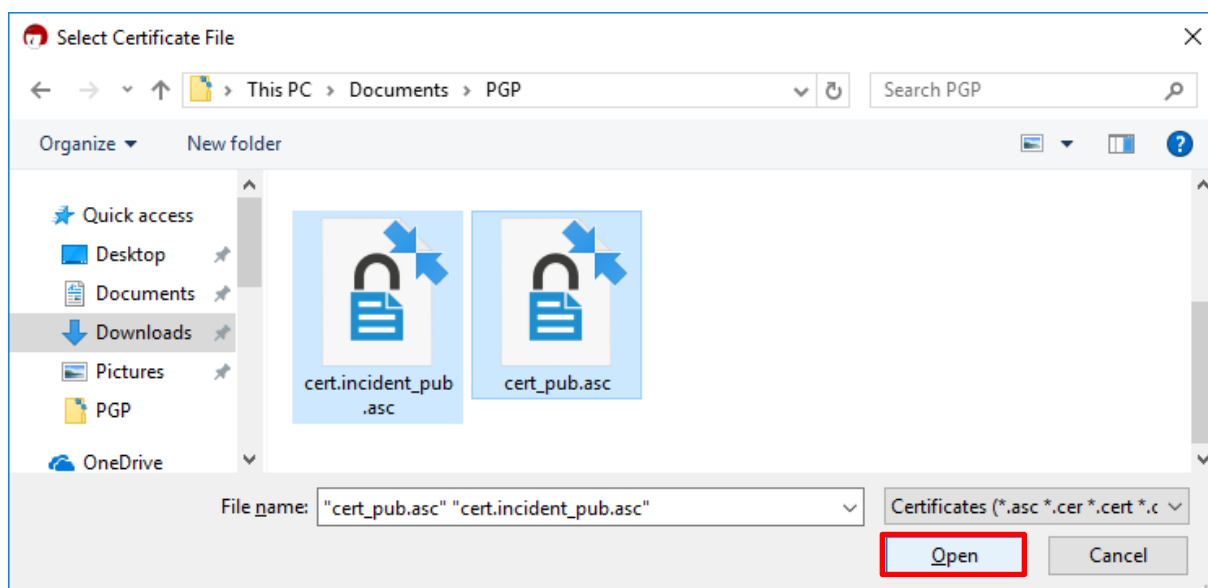
Jestliže jste zadali všechno správně, měl by se v programu Kleopatra objevit Váš nově vytvořený klíčový pár, obsahující soukromý a veřejný klíč.

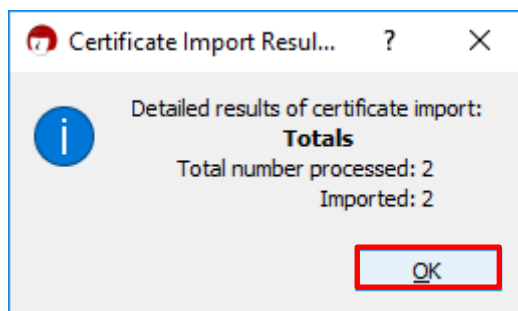
## Import PGP certifikátů do aplikace Kleopatra

Jste-li již majitelem vlastního páru PGP klíčů, můžete je jednoduše nainportovat „File“ -> „Import...“. Dále je potřeba nainportovat veřejné PGP klíče příjemce, kterým je v našem ukázkovém případě GovCERT.CZ. Tyto veřejné klíče lze stáhnout na našich webových stránkách [www.govcert.cz](http://www.govcert.cz), viz výše.

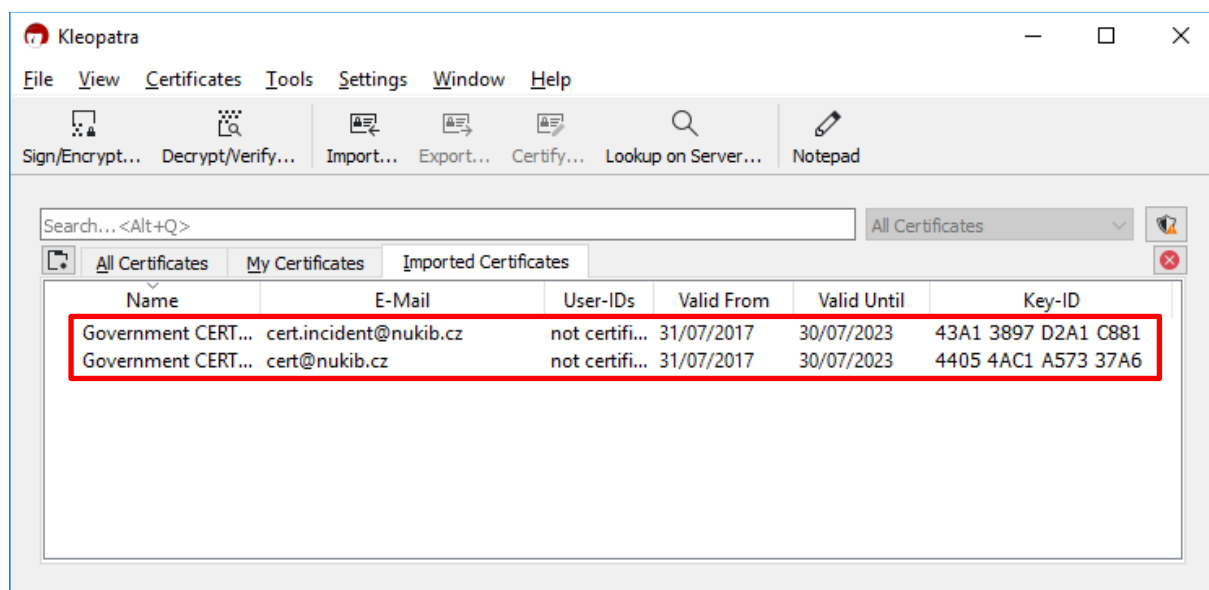


Pro import veřejných klíčů příjemců postupujte obdobně, zvolte „File“ -> „Import...“, nebo klikněte na stejnojmennou ikonku pod hlavním menu aplikace a vyberete příslušné soubory. Potvrďte stisknutím „Otevřít“. Nakonec v malém okně Certificate Import Resolution stiskněte „OK“.





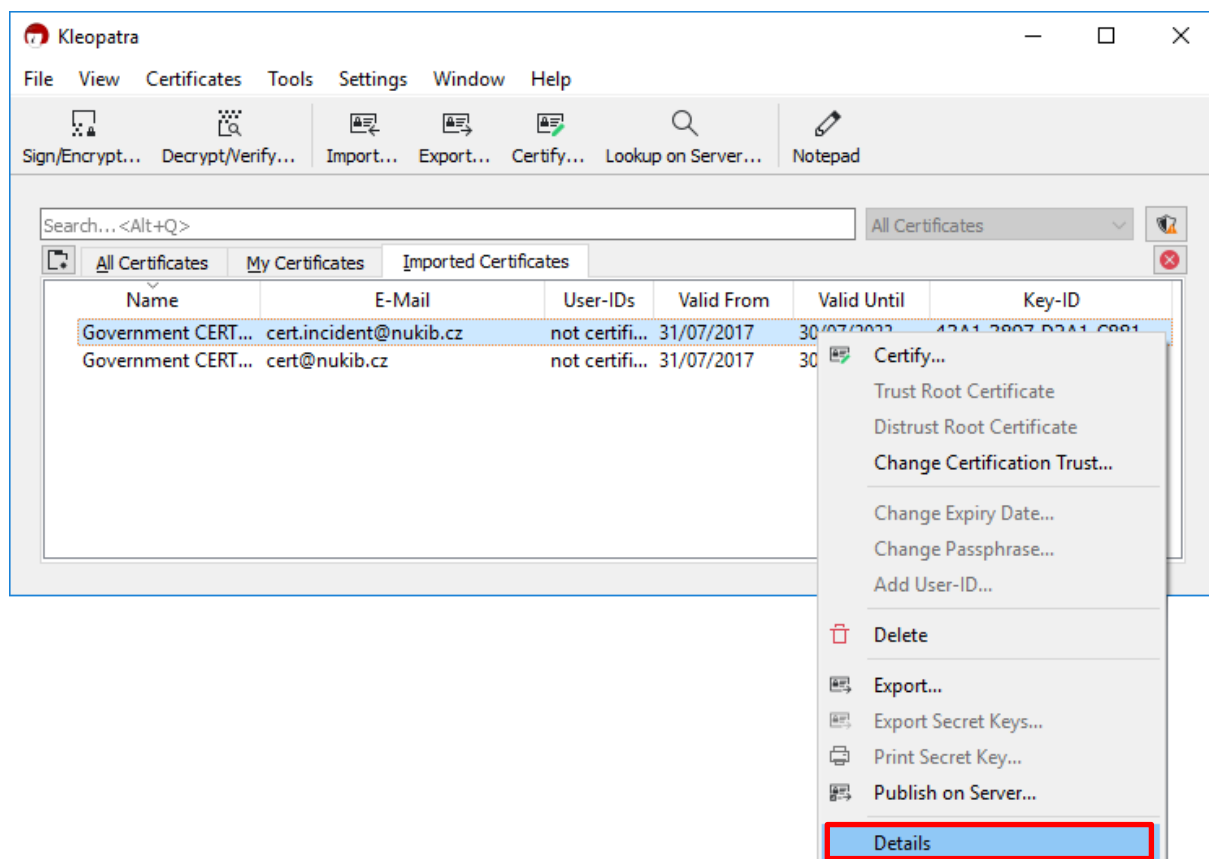
V tuto chvíli byste měli mít v aplikaci Kleopatra v pořádku nainportovány veřejné klíče.





## Kontrola PGP certifikátů

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



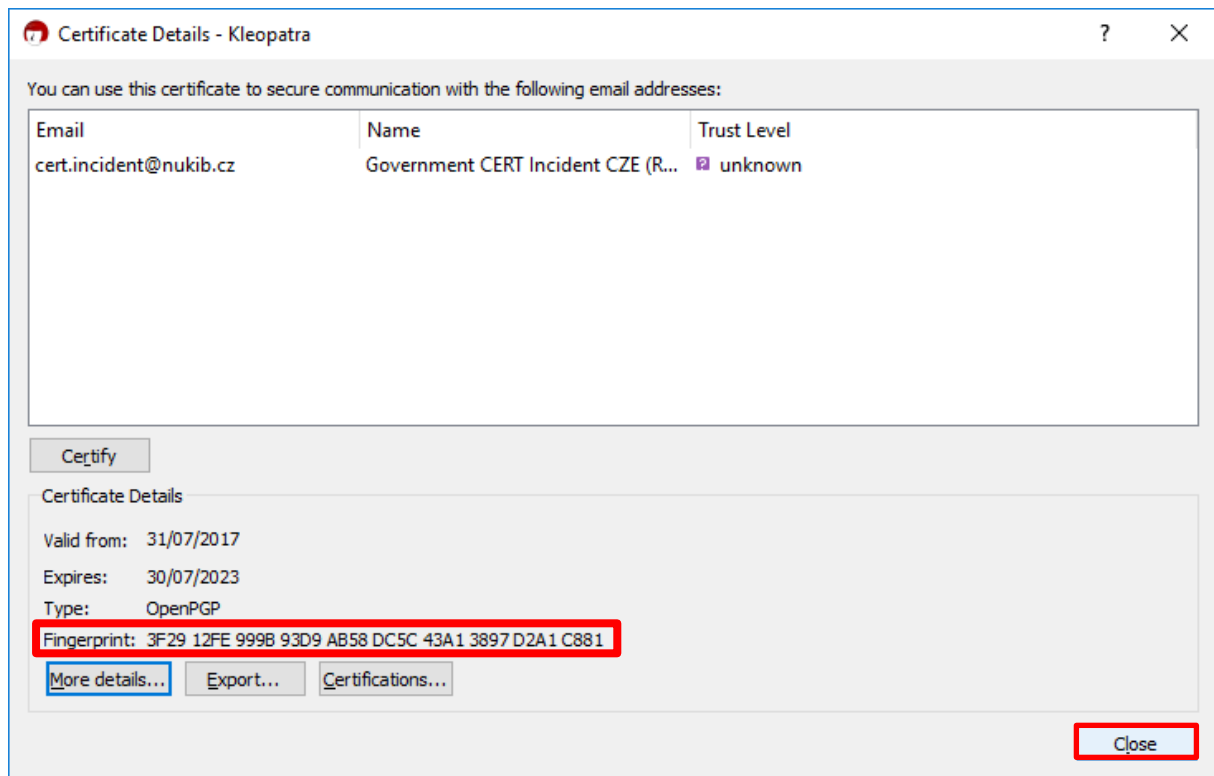
V poli „*fingerprint*“ by se měly nacházet tyto hodnoty:

3F29 12FE 999B 93D9 AB58 DC5C 43A1 3897 D2A1 C881

pro [cert.incident@nukib.cz](mailto:cert.incident@nukib.cz)

F60C 0622 EE75 52C9 7EE5 E9F8 4405 4AC1 A573 37A6

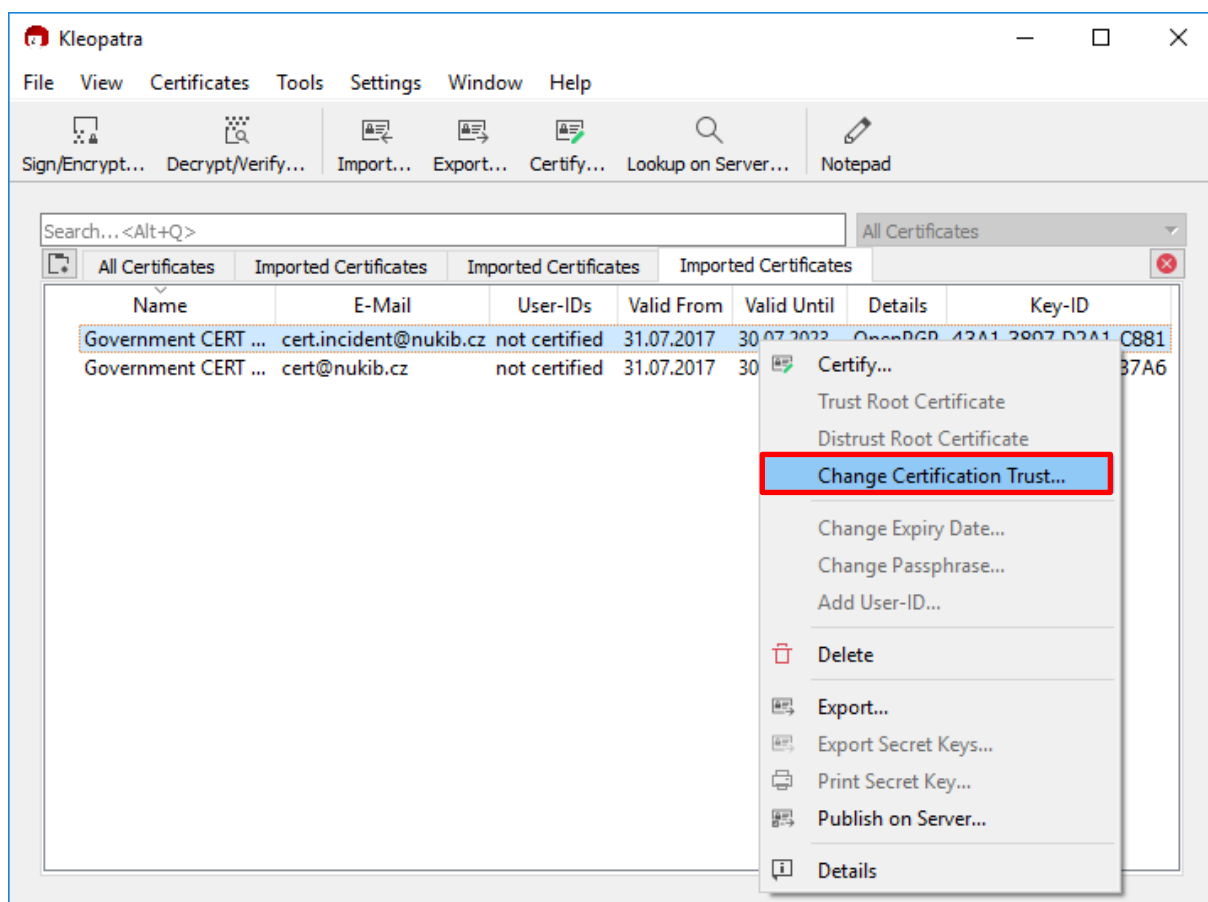
pro [cert@nukib.cz](mailto:cert@nukib.cz)

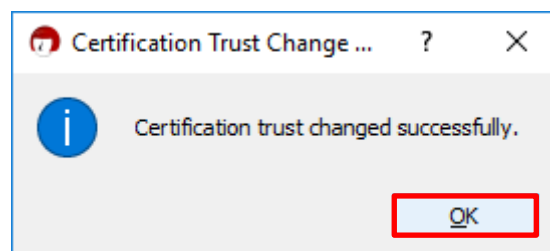
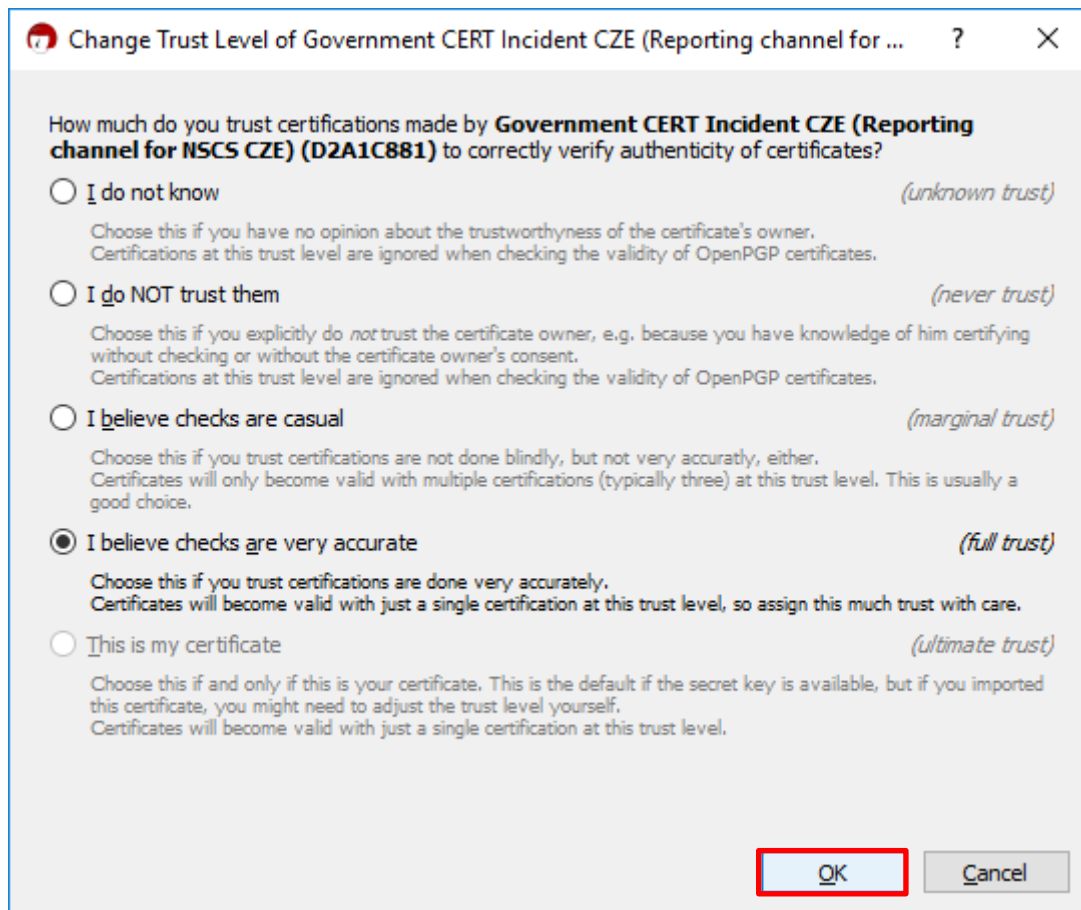


Pokud tyto hodnoty souhlasí, okno zavřete stiskem tlačítka „Close“.

## Nastavení důvěryhodnosti certifikátů

Po ověření je nutné, abyste nastavili u jednotlivých certifikátů jejich 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 „*OK*“.

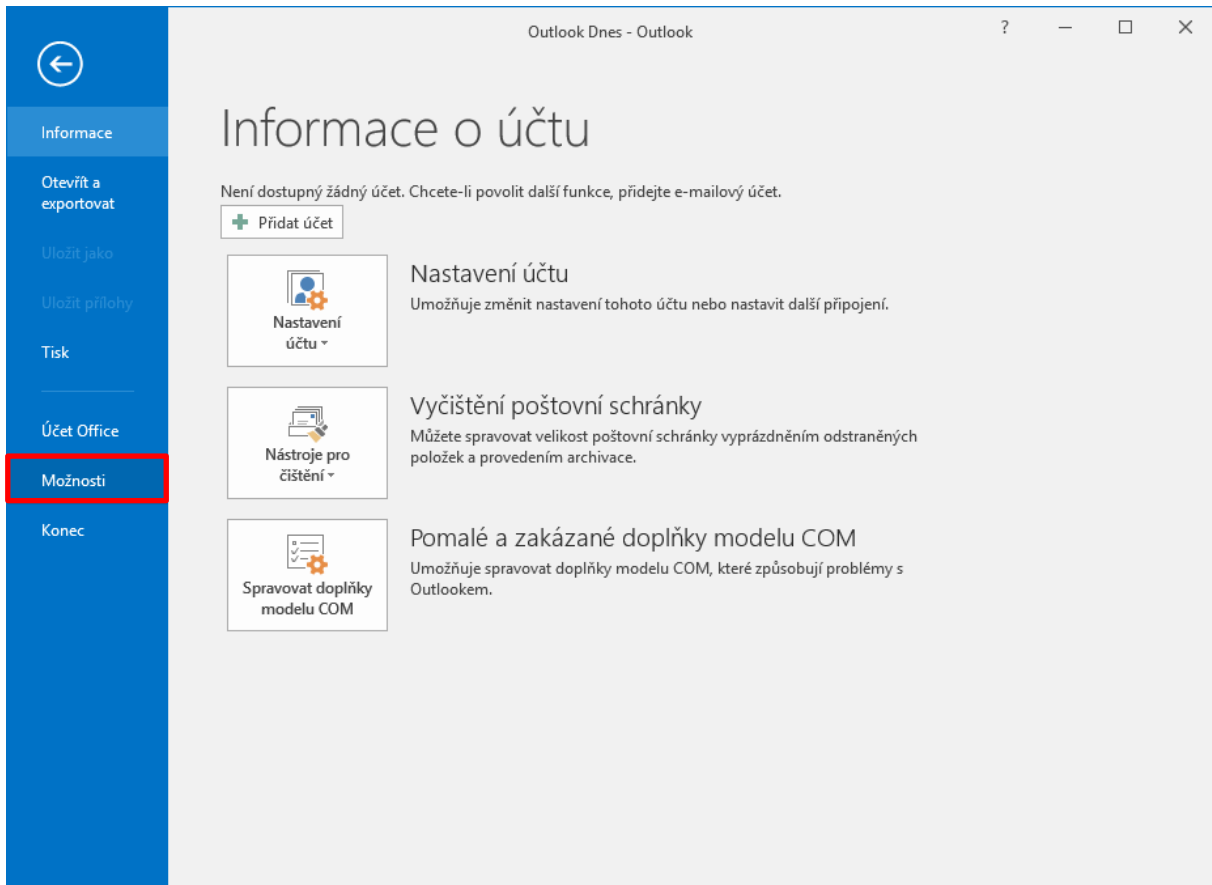




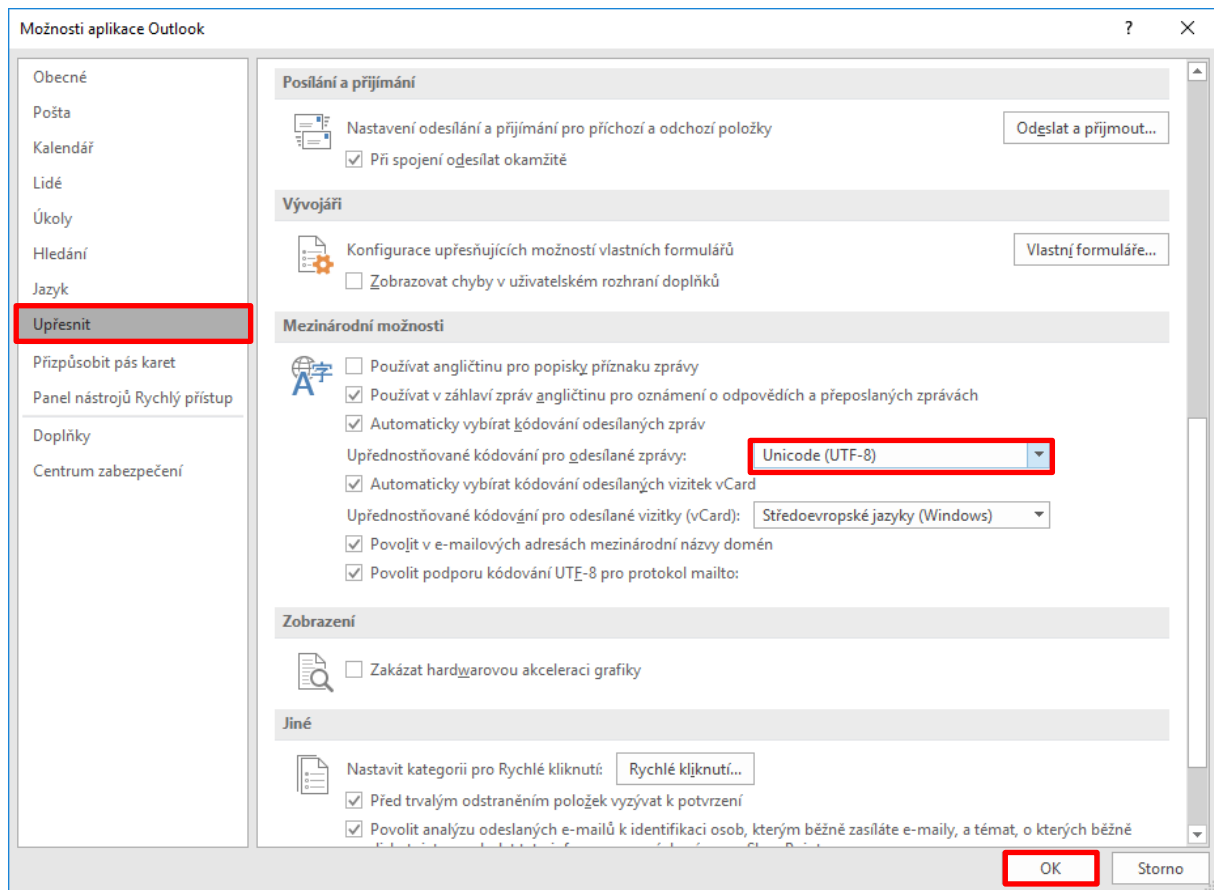
Aplikaci Kleopatra lze nyní vypnout.

## Nastavení kódování pro odesílané zprávy v MS Outlook

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

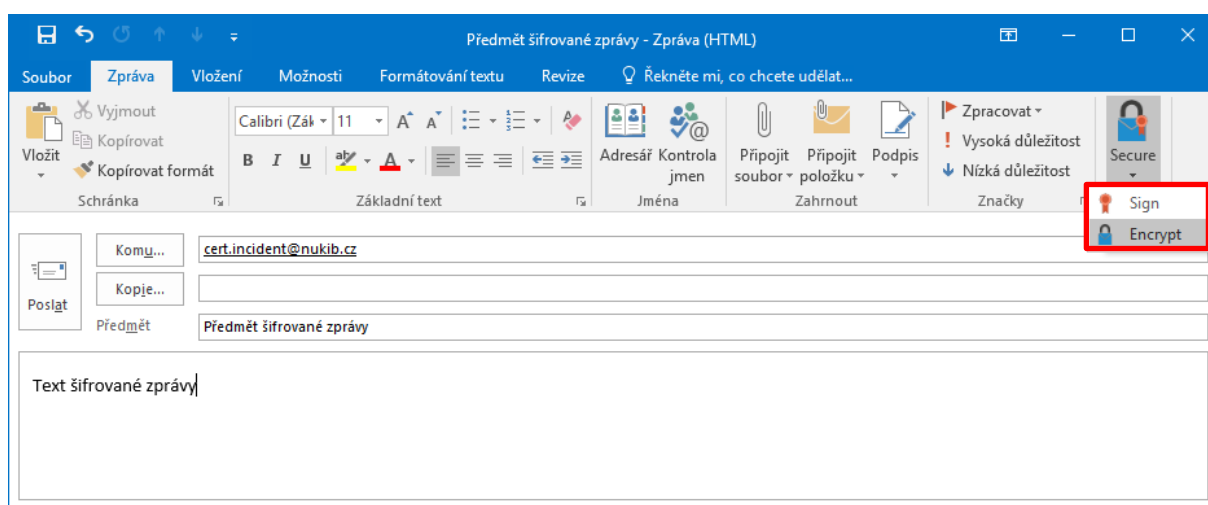


V záložce „*Upřesnit*“ je v části označené jako „*Mezinárodní možnosti*“ nutno změnit položku „*Upřednostňované kódování pro odesílané zprávy*“. Zde nastavte hodnotu „*Unicode (UTF-8)*“.



## 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 například 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.

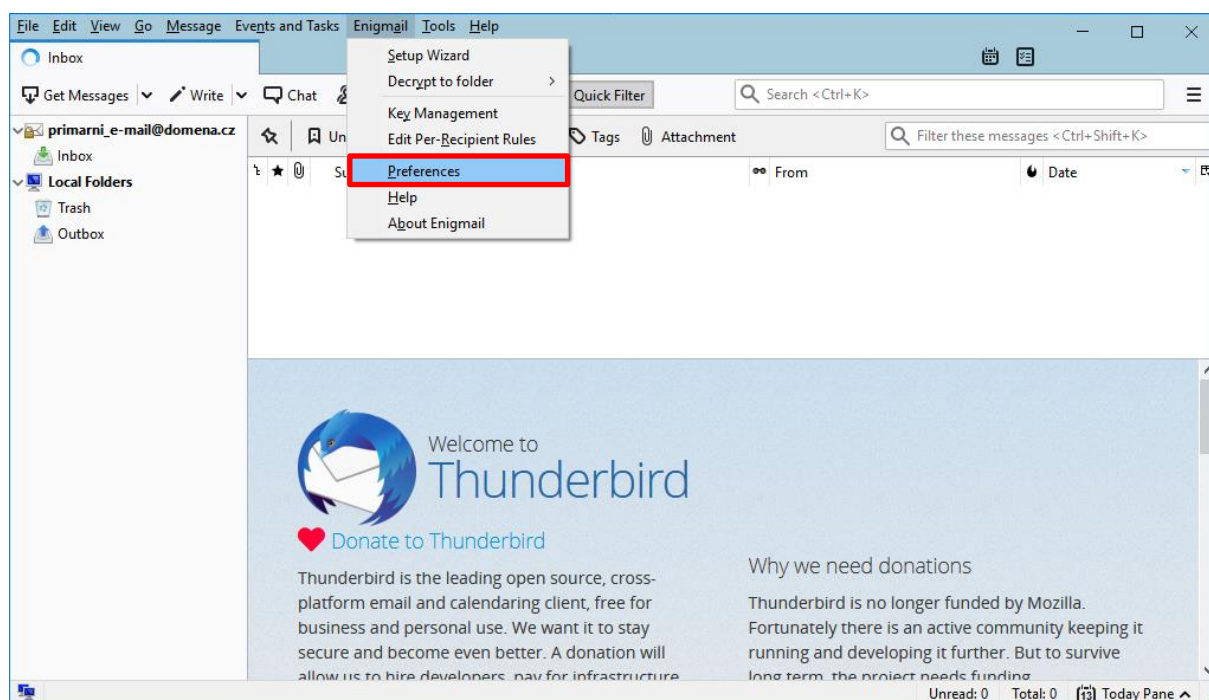


Nyní je již možno e-mail odeslat. Pokud byla zvolena možnost „Sign“, bude před jeho odesláním požádáno o zadání hesla od Vašeho soukromého klíče. V případě, že databáze v aplikaci Kleopatra neobsahuje veřejný klíč odpovídající e-mailové adrese příjemce, budete před odesláním vyzváni k výběru odpovídajícího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

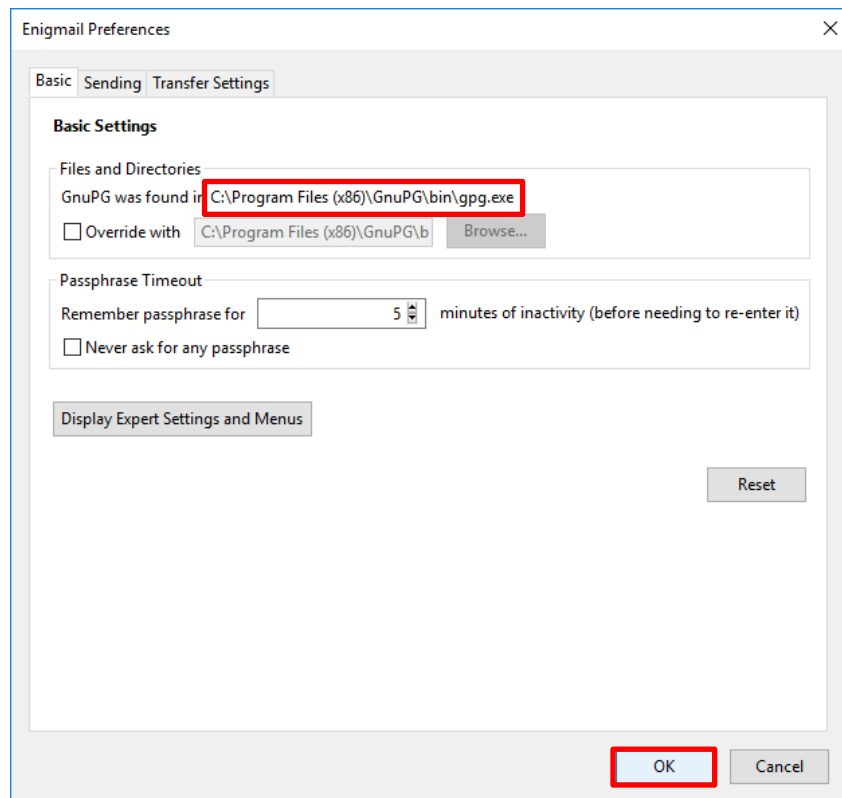
## Instalace PGP pro Mozilla Thunderbird

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 potřeba ještě 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 -> Doplněk -> 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“. Tuto položku rozklikněte a v položce „Preferences“ (Předvolby...) v záložce „Basic“ (Základní) zkontrolujte, zda se nastavila správná cesta k místu, kam jste nainstalovali aplikaci GnuPG.

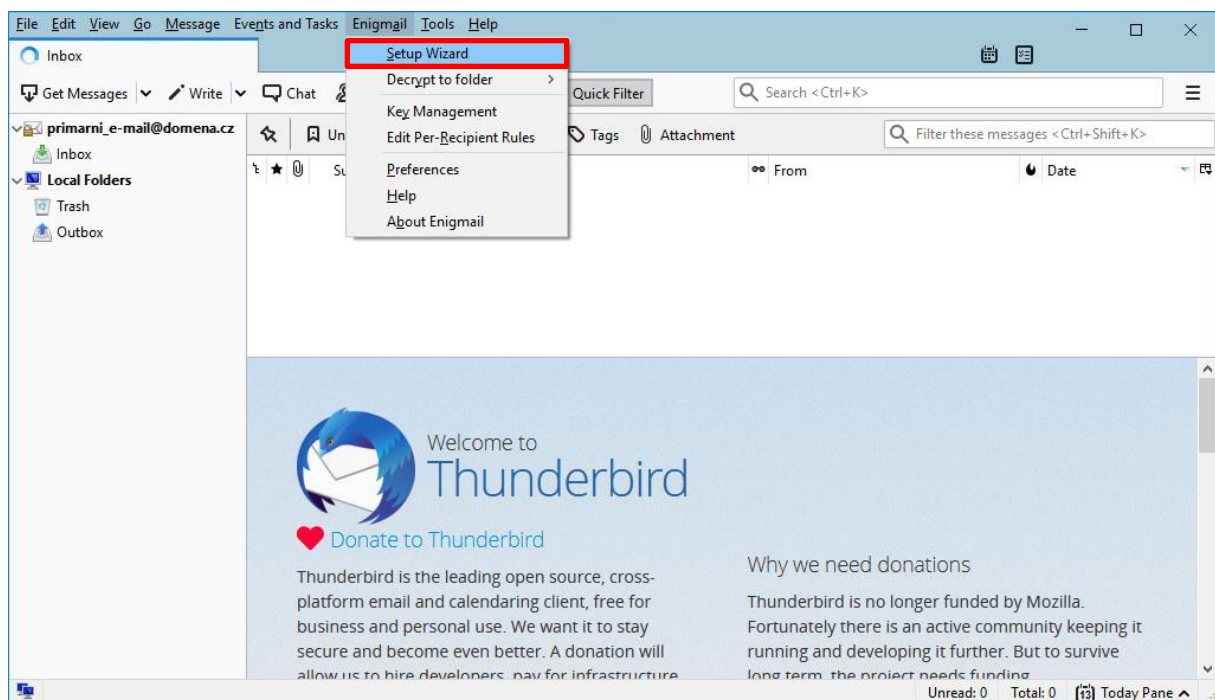




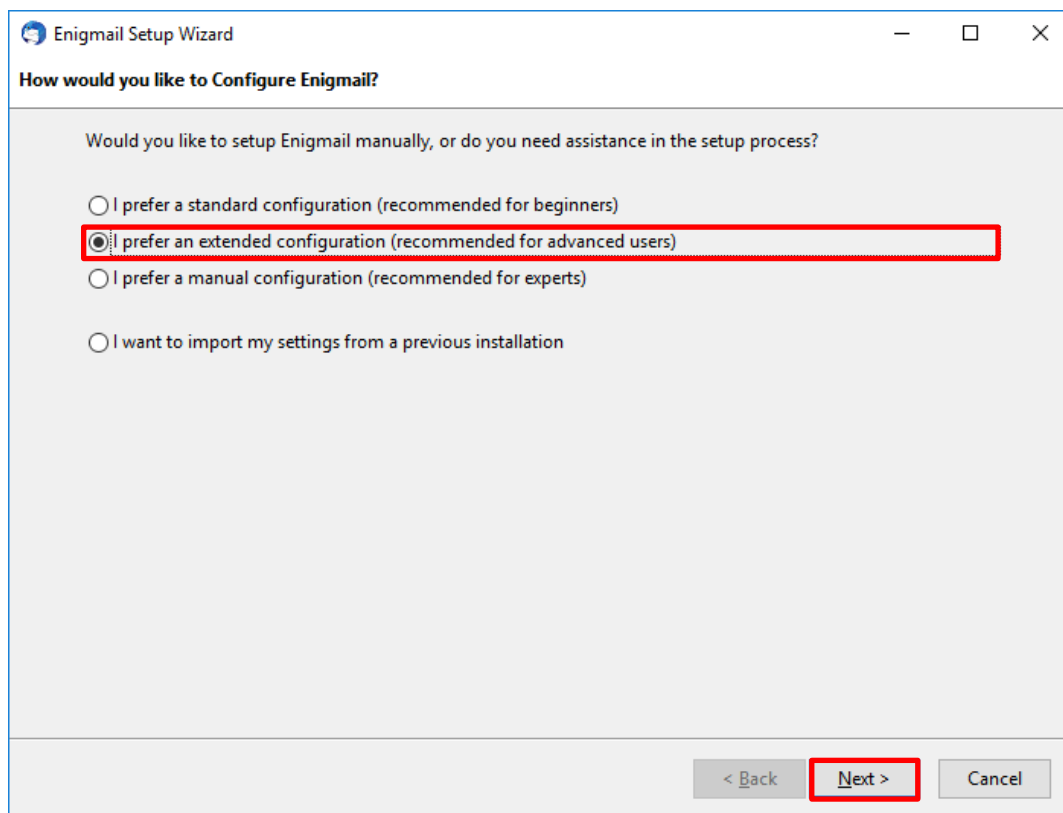


Pokud zde není uvedena žádná cesta, nebo je uvedena nesprávná cesta instalace aplikace, je nutno ji správně doplnit či opravit.

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 vložení existujících klíčů, či vytvoření nových. Potvrďte stiskem „Next“ (Další).



Enigmail Setup Wizard

How would you like to Configure Enigmail?

Would you like to setup Enigmail manually, or do you need assistance in the setup process?

I prefer a standard configuration (recommended for beginners)

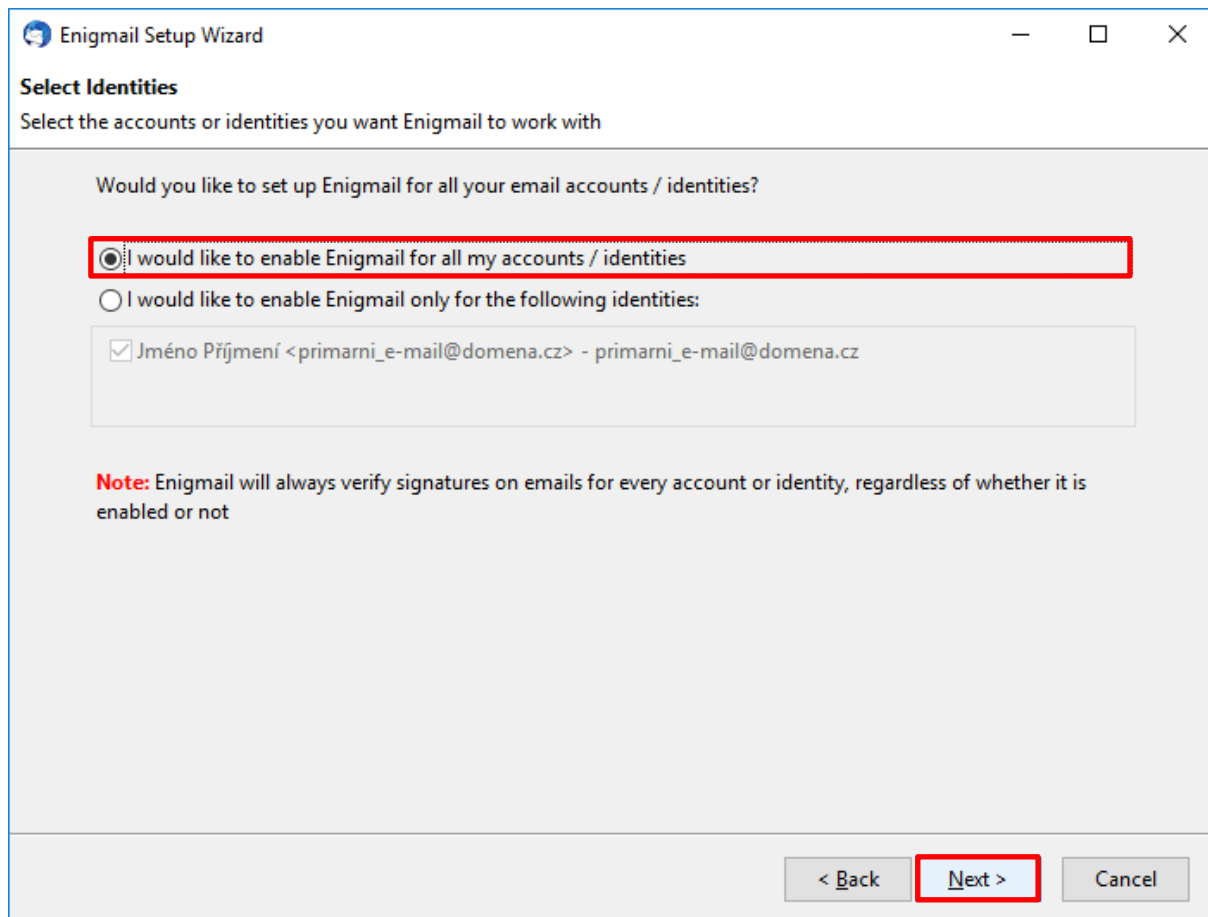
I prefer an extended configuration (recommended for advanced users)

I prefer a manual configuration (recommended for experts)

I want to import my settings from a previous installation

< Back   Next >   Cancel

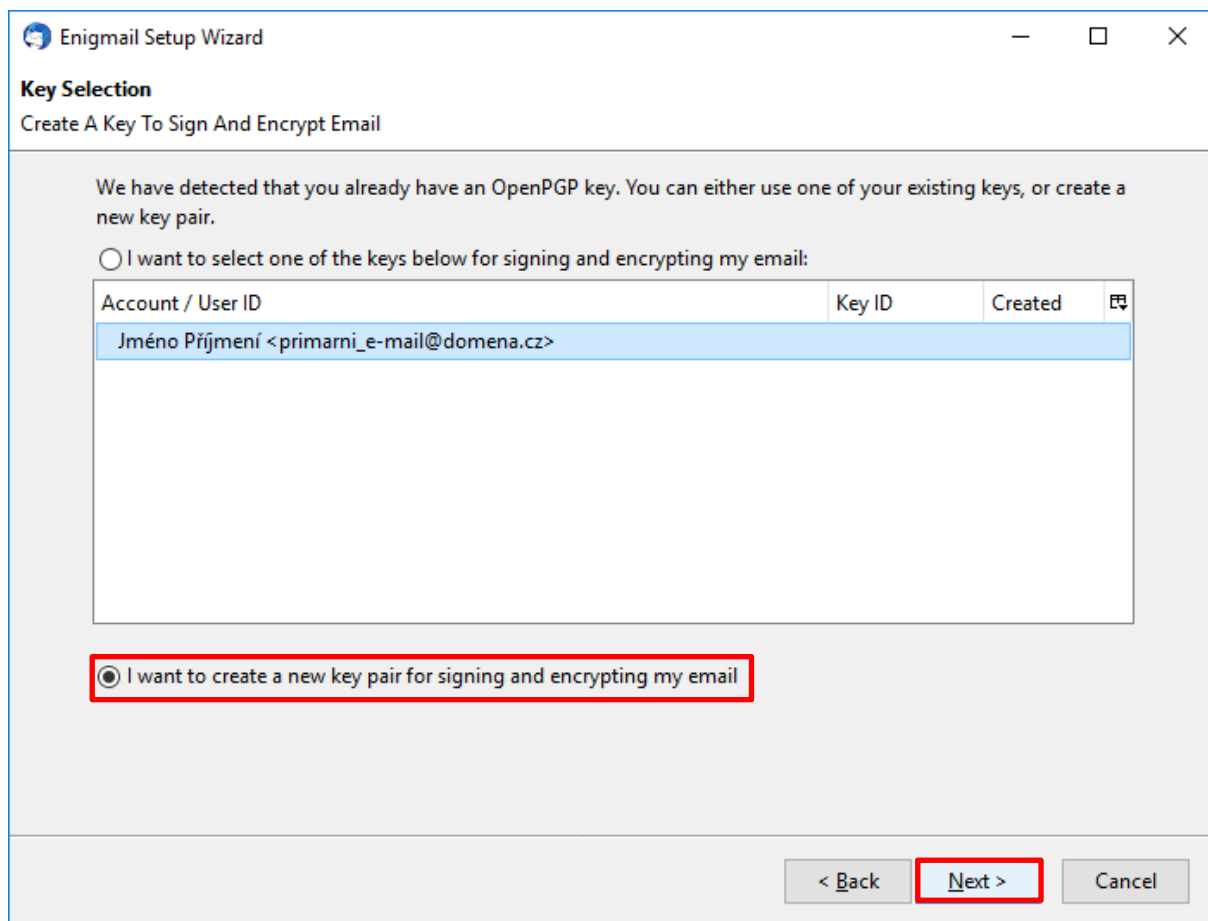
Dále je potřeba zvolit, pro které Vaše e-mailové účty chcete používání PGP certifikátů nastavit. Pokud používáte více účtů, lze vybrat, se kterými konkrétními identitami bude Enigmail pracovat. V případě, že používáte pouze jeden, nebo chcete pravidla nastavit pro všechny e-mailové účty, vyberte první 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 nainportovat již existující (v tom případě přeskočte prosím následující sekci na část Import PGP certifikátů).

## Vytvoření vlastního PGP certifikátu

Pokud ještě nemáte vlastní pár klíčů, nebo si přejete vytvořit nový, 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 na „Next“.



V dalším kroku si musíte pro vybraný pár klíčů zvolit do příslušných polí heslo a potvrdit stiskem na „Next“. Při tvorbě bezpečného hesla je vhodné aplikovat pravidla [best-practise](#).

Enigmail Setup Wizard

### Create Key

Create a new Key Pair

This dialog will create a pair of keys:  
Your **public key** is **for others** to send you encrypted emails. You can distribute it to everybody.  
Your **secret key** is **for you** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your secret key. It prevents misuse of your secret key. The passphrase should contain several words and at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Account / User ID:  
Jméno Příjmení <primarni\_e-mail@domena.cz> - primarni\_e-mail@domena.cz

Passphrase  
●●●●●●●●

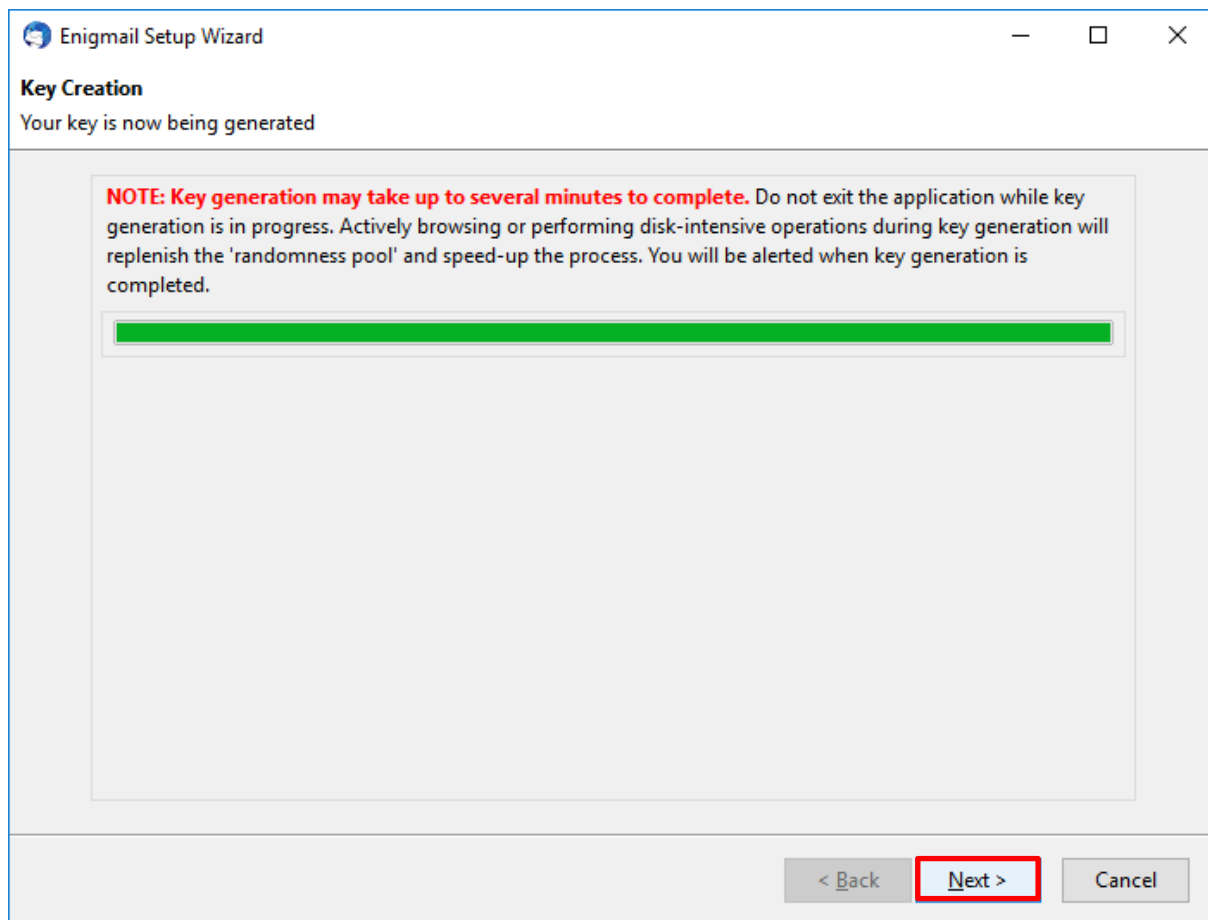
Please confirm your passphrase by typing it again  
●●●●●●●●

Passphrase quality:  
■■■■■■■■

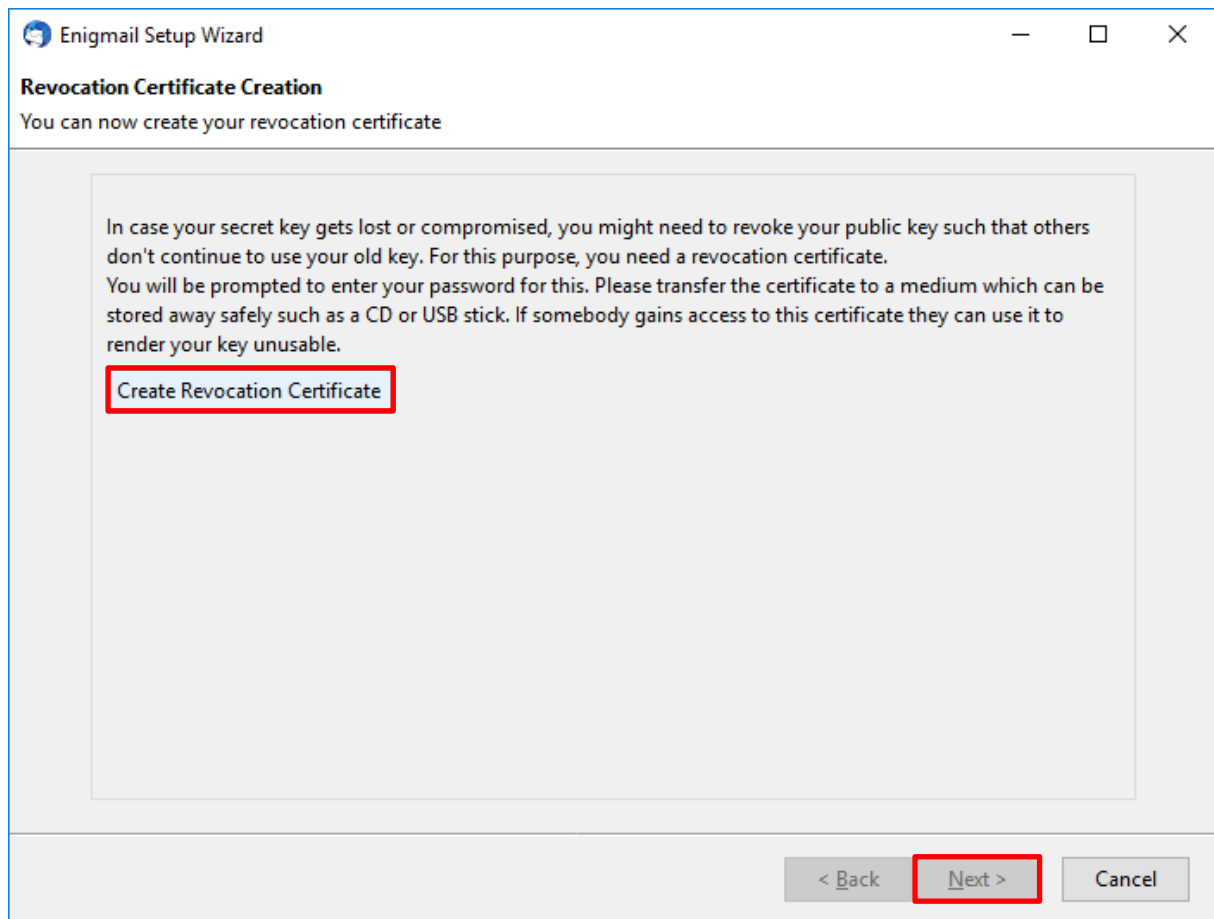
Remember passphrase for 5 minutes of inactivity (before needing to re-enter it)

< Back **Next >** Cancel

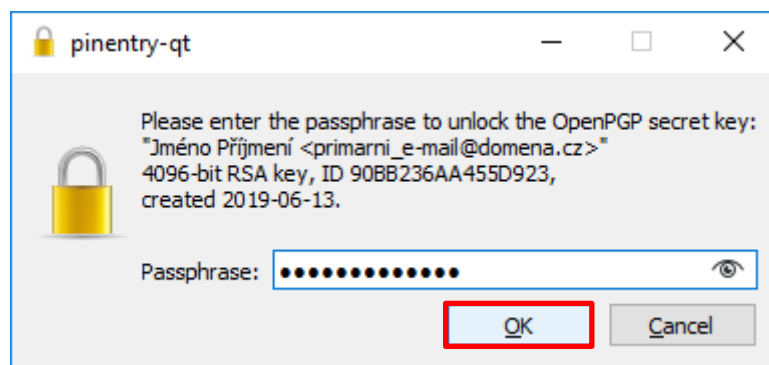
Rozeběhne se proces generování klíčů, jehož rychlost (entropii) lze podpořit stisknutím libovolných kláves, či manipulací s jinými aplikacemi.



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

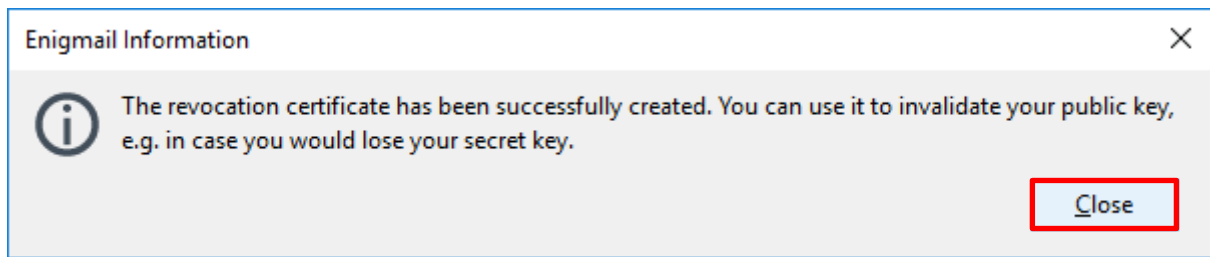


Dále jste vyzváni, abyste zadali heslo, které jste zvolili v předchozím kroku a vzápětí k uložení revokačního certifikátu.



V průběhu ukládání revokačního certifikátu vyberte vhodnou lokaci, kde jej v případě potřeby snadno dohledáte a potvrďte stiskem „Save“ (Uložit).

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

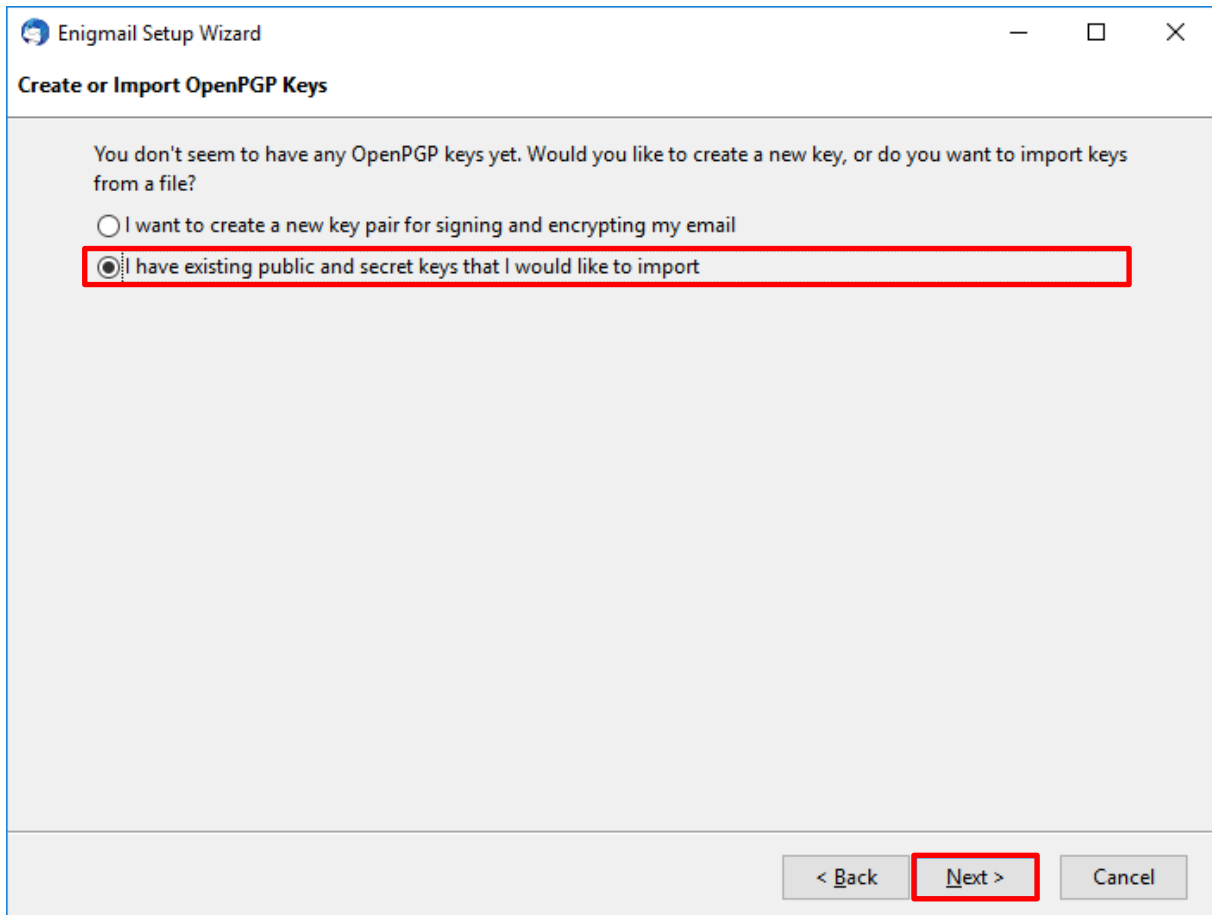


Po potvrzení upozornění pokračujte stisknutím „Next“ v okně Setup Wizard a potvrďte jeho dokončení „Close“.



## 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 zadat do příslušných polí cestu k Vašemu veřejnému a soukromému klíči. Potvrďte „Next“.

Enigmail Setup Wizard

**Import OpenPGP Keys**  
Specify the files to import

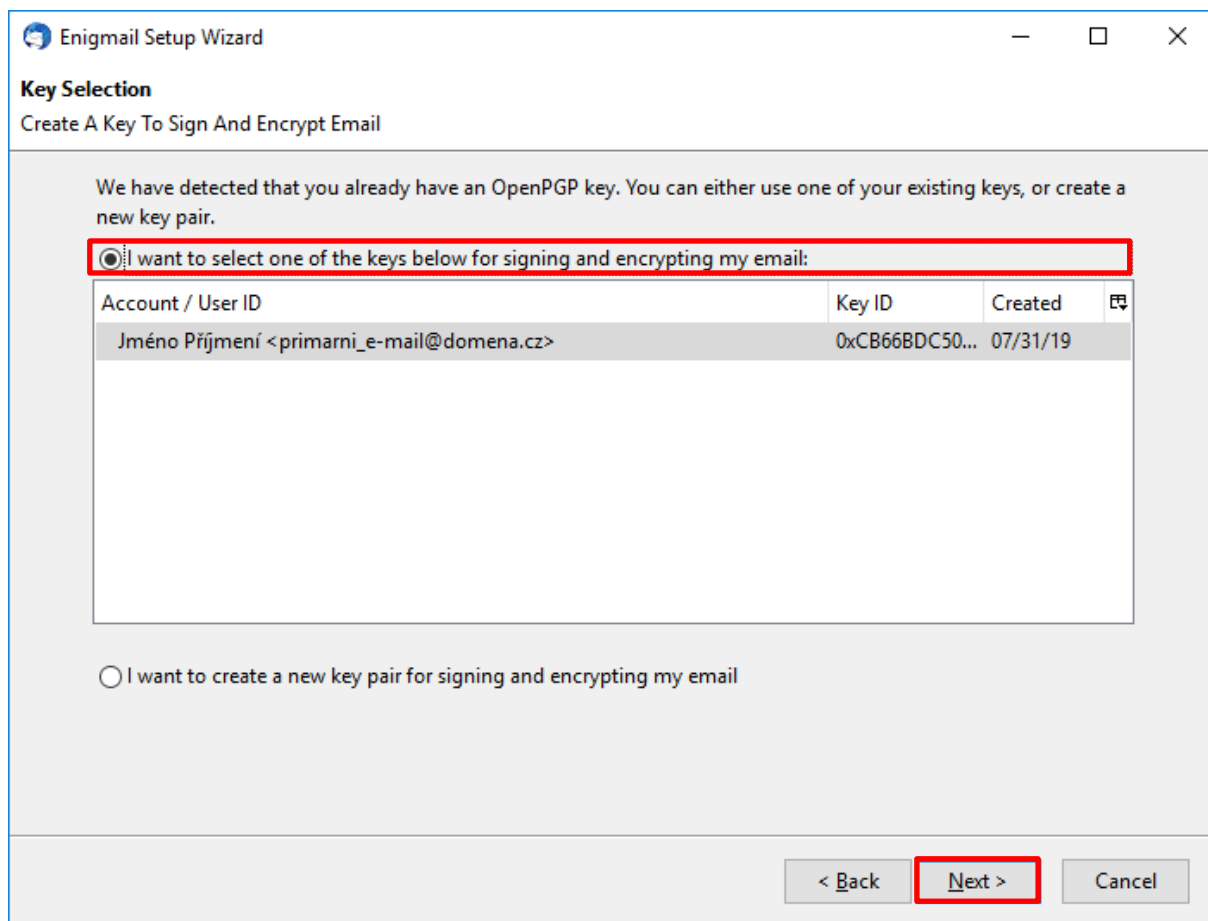
Please specify the files containing the public and the secret keys to import. The entry for secret keys can be left empty if the first file contains both secret and public keys.

Public key file  Browse...

Secret key file  Browse...

< Back **Next >** Cancel

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“.



**Enigmail Setup Wizard**

**Key Selection**  
Create A Key To Sign And Encrypt Email

We have detected that you already have an OpenPGP key. You can either use one of your existing keys, or create a new key pair.

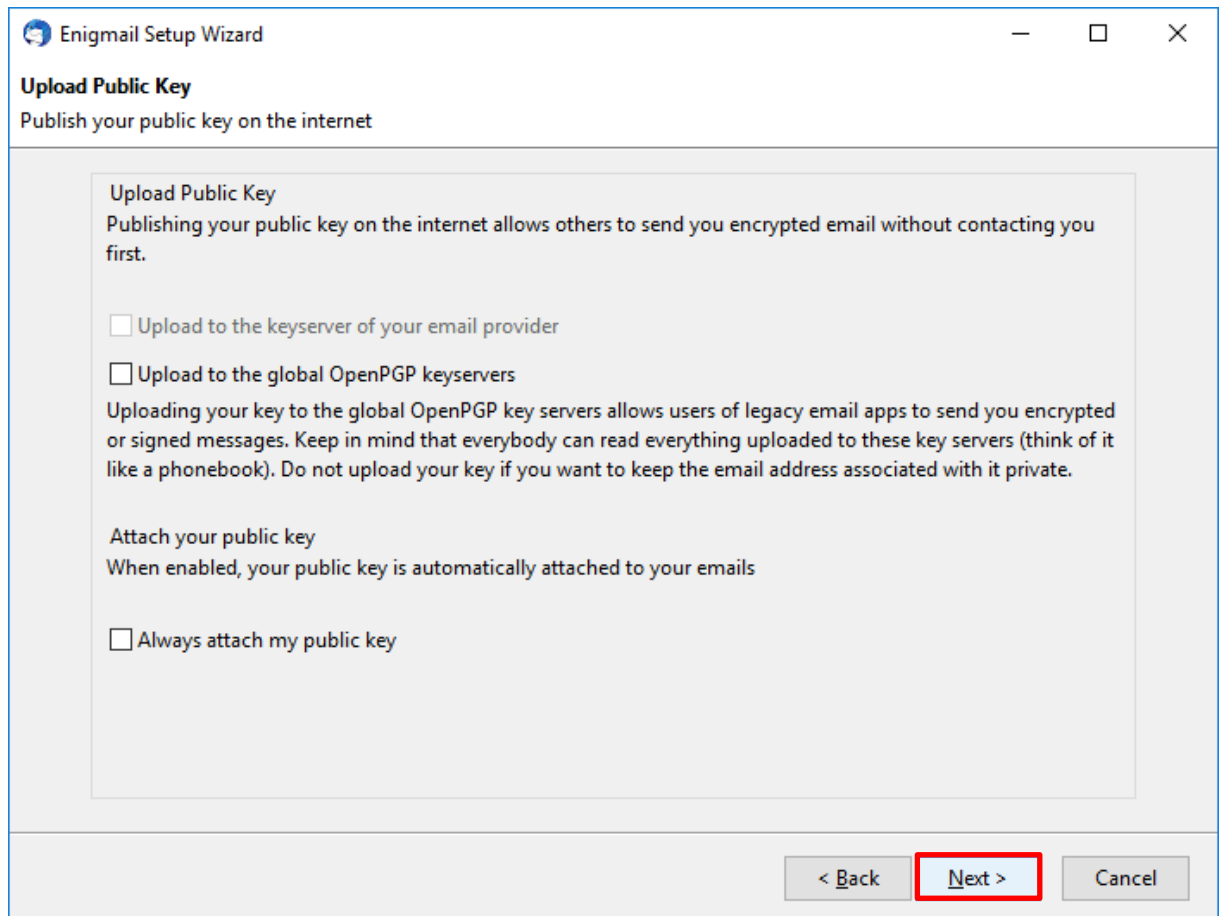
I want to select one of the keys below for signing and encrypting my email:

Account / User ID	Key ID	Created	
Jméno Příjmení <primarni_e-mail@domena.cz>	0xCB66BDC50...	07/31/19	

I want to create a new key pair for signing and encrypting my email

< Back **Next >** Cancel

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.



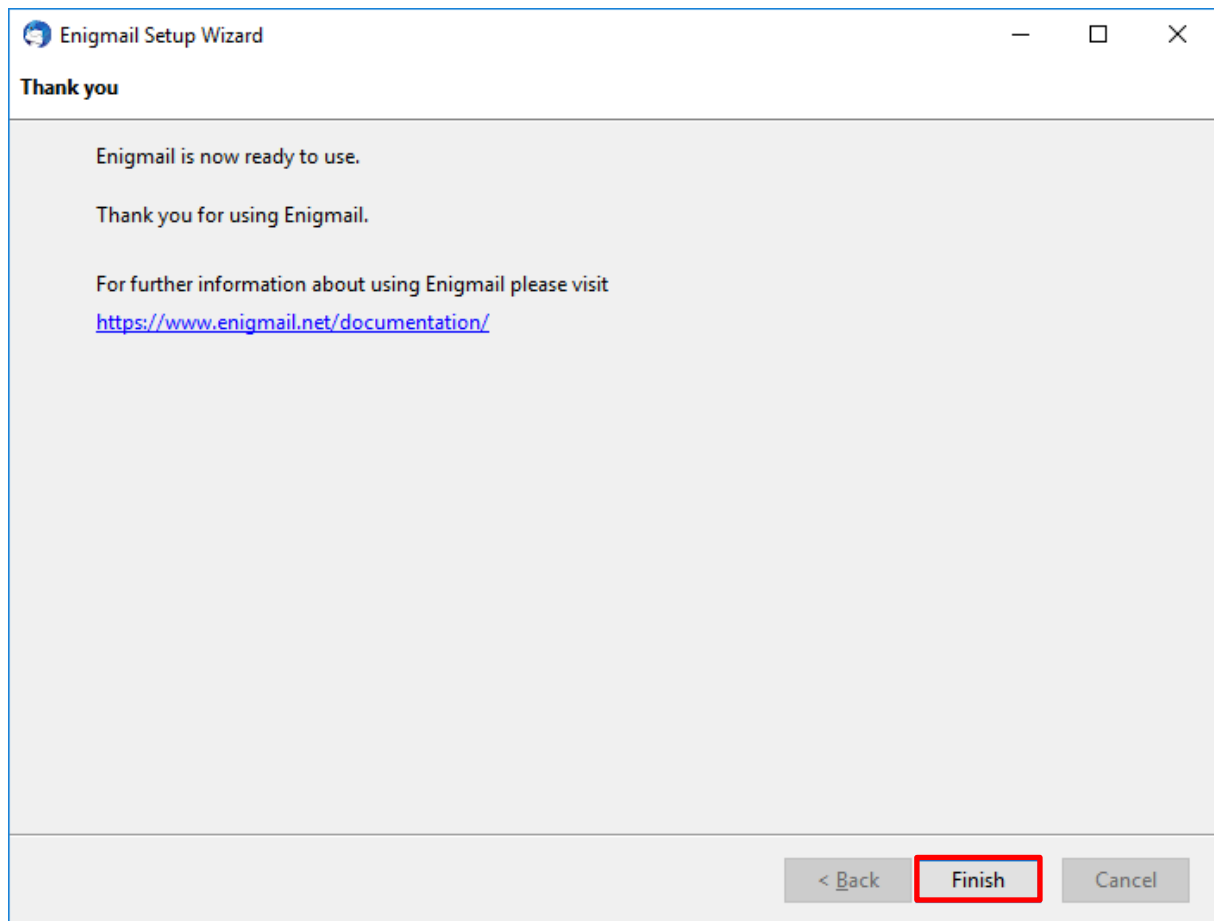
The screenshot shows a window titled "Enigmail Setup Wizard" with a standard Windows title bar (minimize, maximize, close buttons). The main heading is "Upload Public Key" with the subtitle "Publish your public key on the internet".

The main content area contains the following text and options:

- Upload Public Key**  
Publishing your public key on the internet allows others to send you encrypted email without contacting you first.
- Upload to the keyserver of your email provider
- Upload to the global OpenPGP keyservers  
Uploading your key to the global OpenPGP key servers allows users of legacy email apps to send you encrypted or signed messages. Keep in mind that everybody can read everything uploaded to these key servers (think of it like a phonebook). Do not upload your key if you want to keep the email address associated with it private.
- Attach your public key**  
When enabled, your public key is automatically attached to your emails
- Always attach my public key

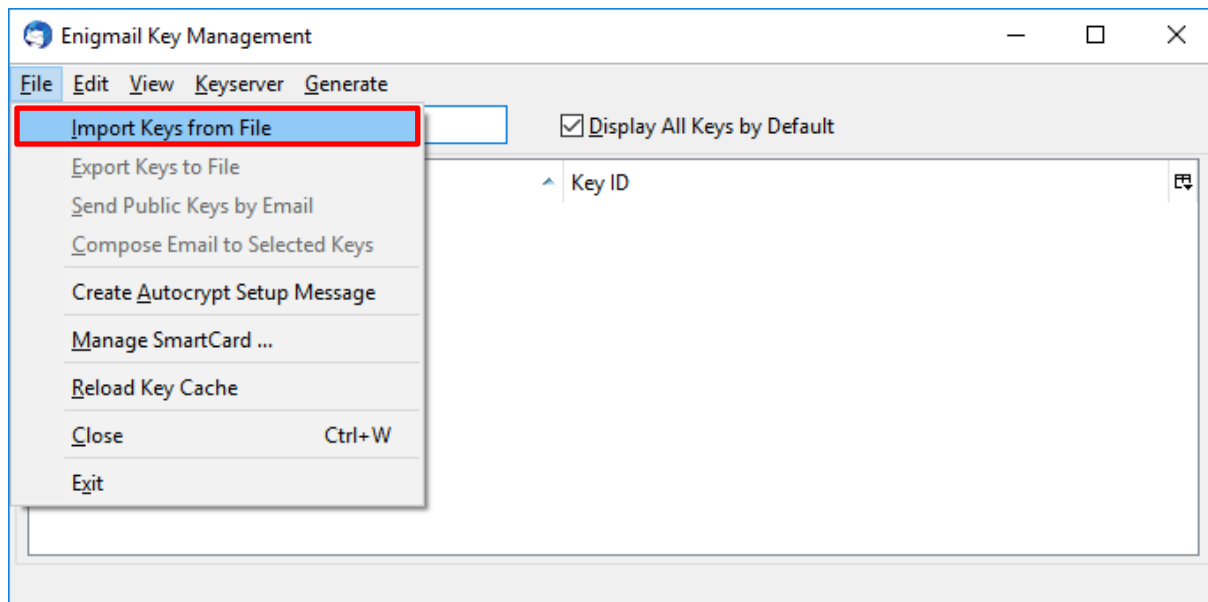
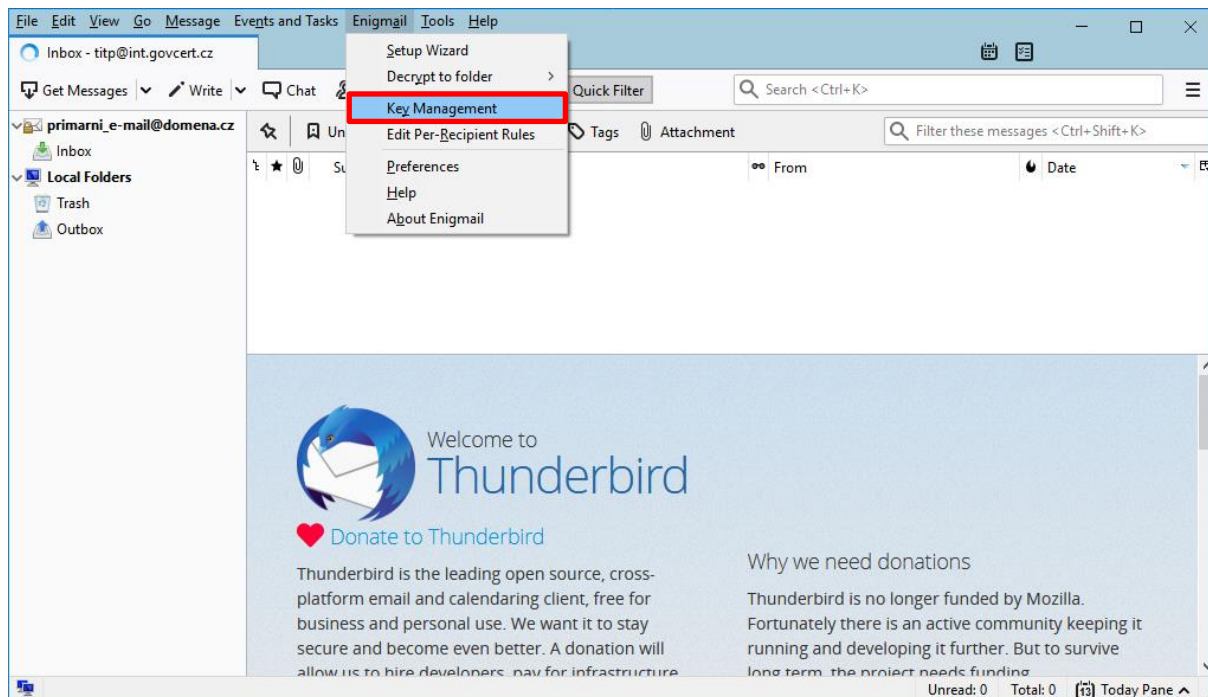
At the bottom right, there are three buttons: "< Back", "Next >" (highlighted with a red rectangle), and "Cancel".

Následně dokončíme nastavení.

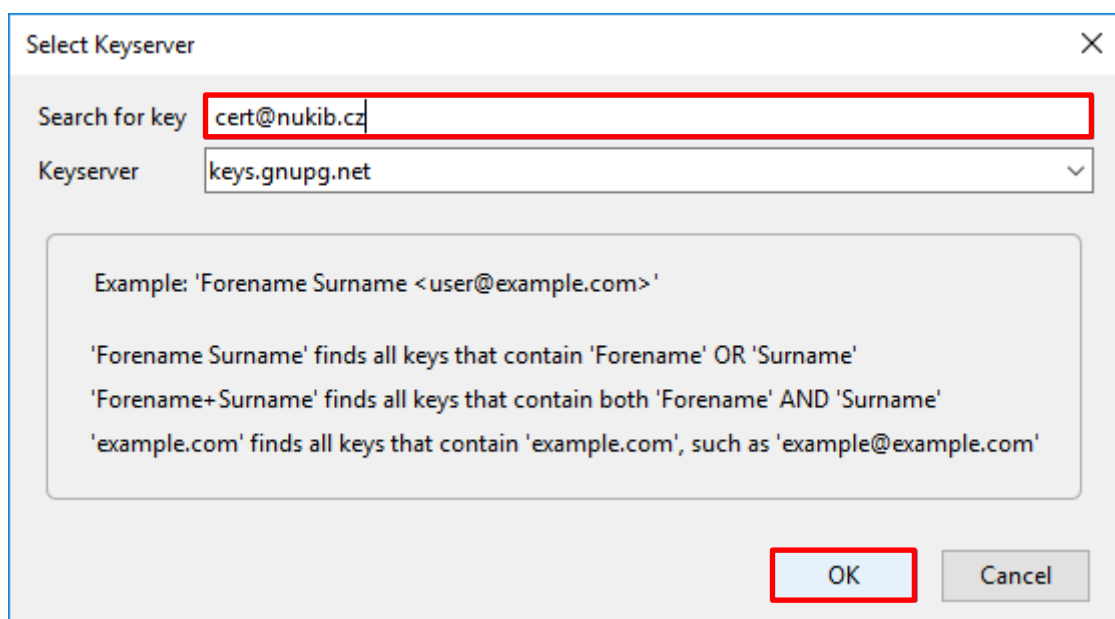
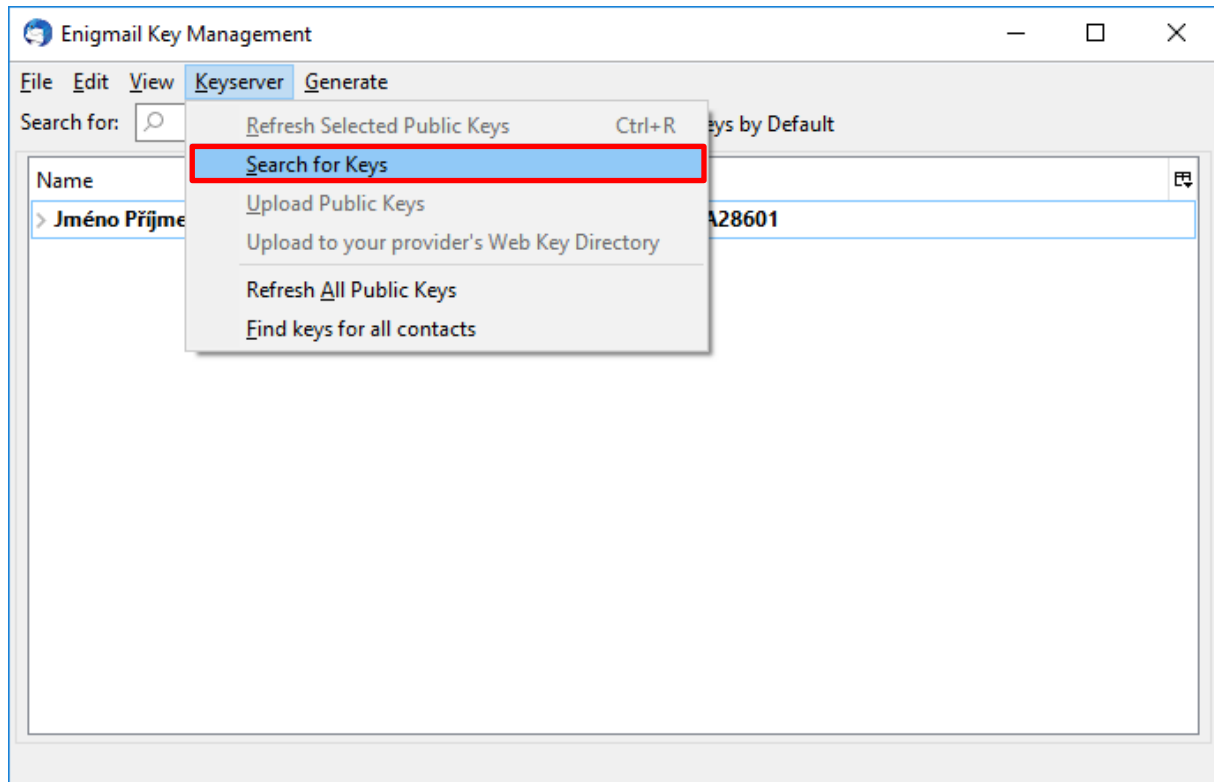


## Import PGP certifikátů příjemců

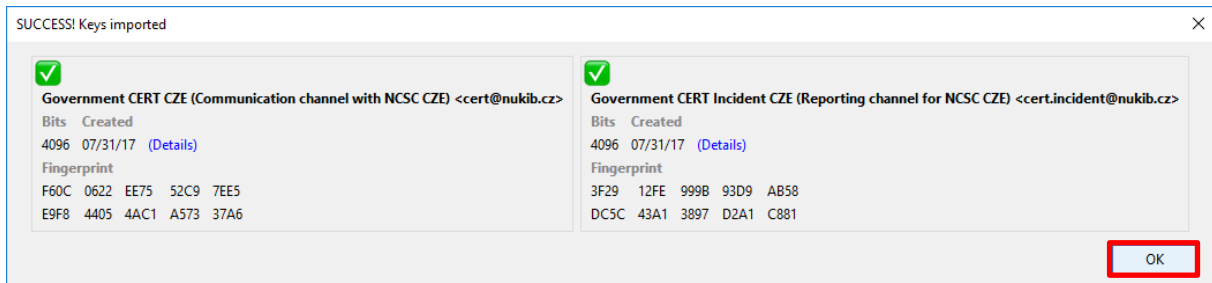
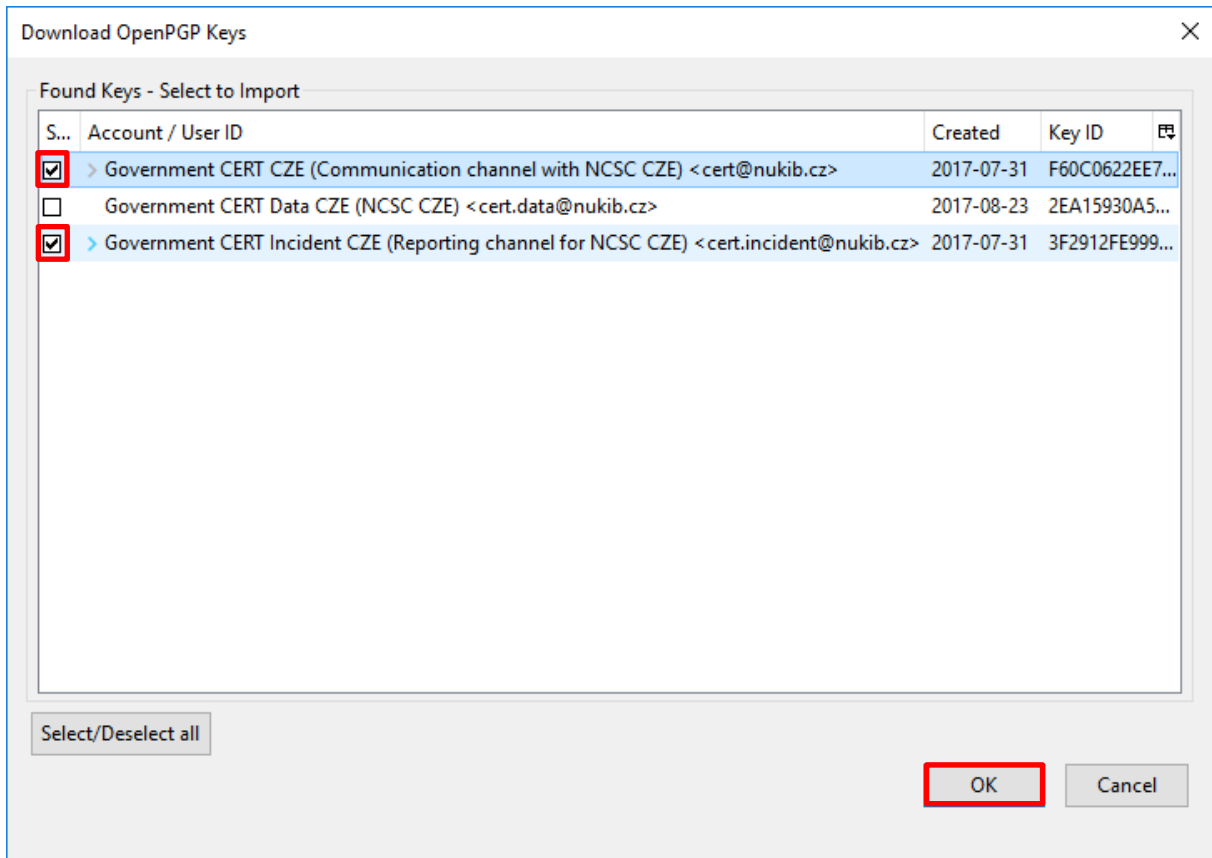
Nyní zbývá nainportovat PGP klíče příjemců, což provedete následně: „Enigmail“ -> „Key Management“ (Správa klíčů). Pokud Vám byly veřejné klíče zaslány e-mailem, nebo jste je stáhli z důvěryhodného zdroje, pokračujte: „File“ -> „Import Keys from File“ (Soubor -> Importovat klíče ze souboru).



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“.

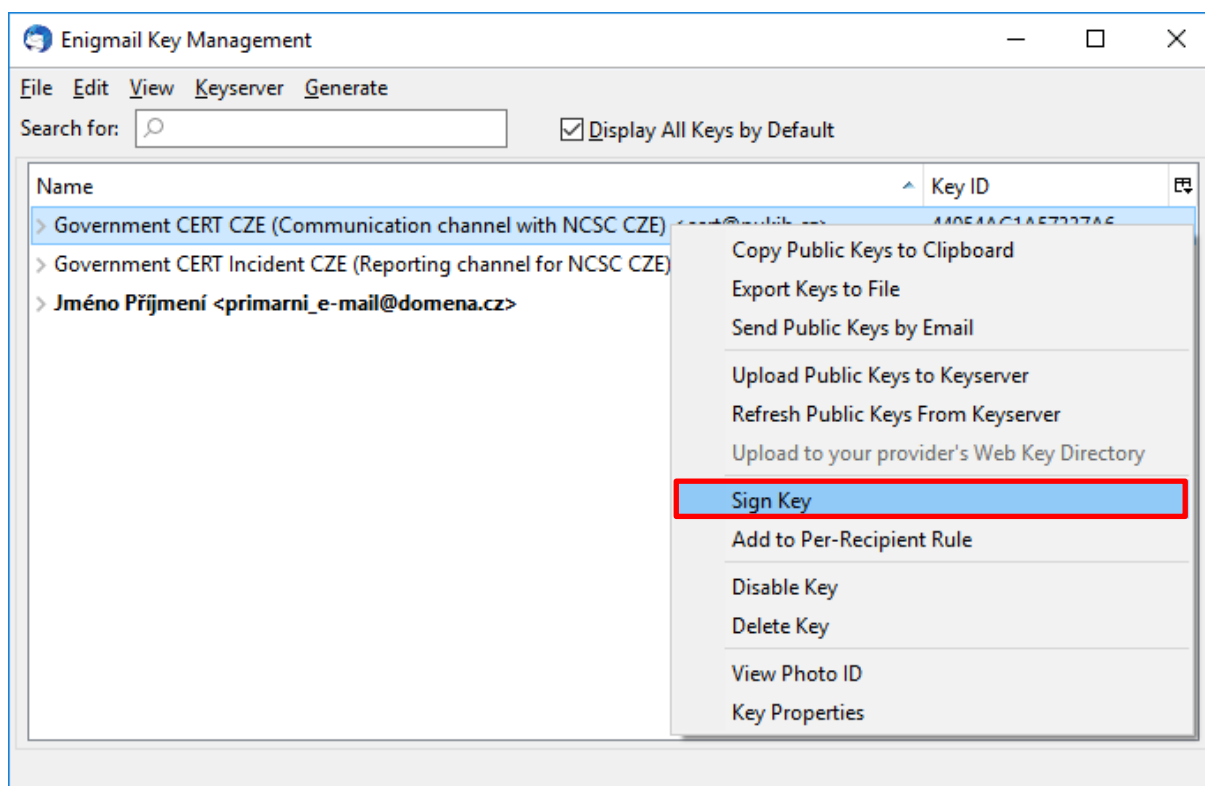


Posléze označte požadované veřejné klíče, které ze serveru stáhnete.

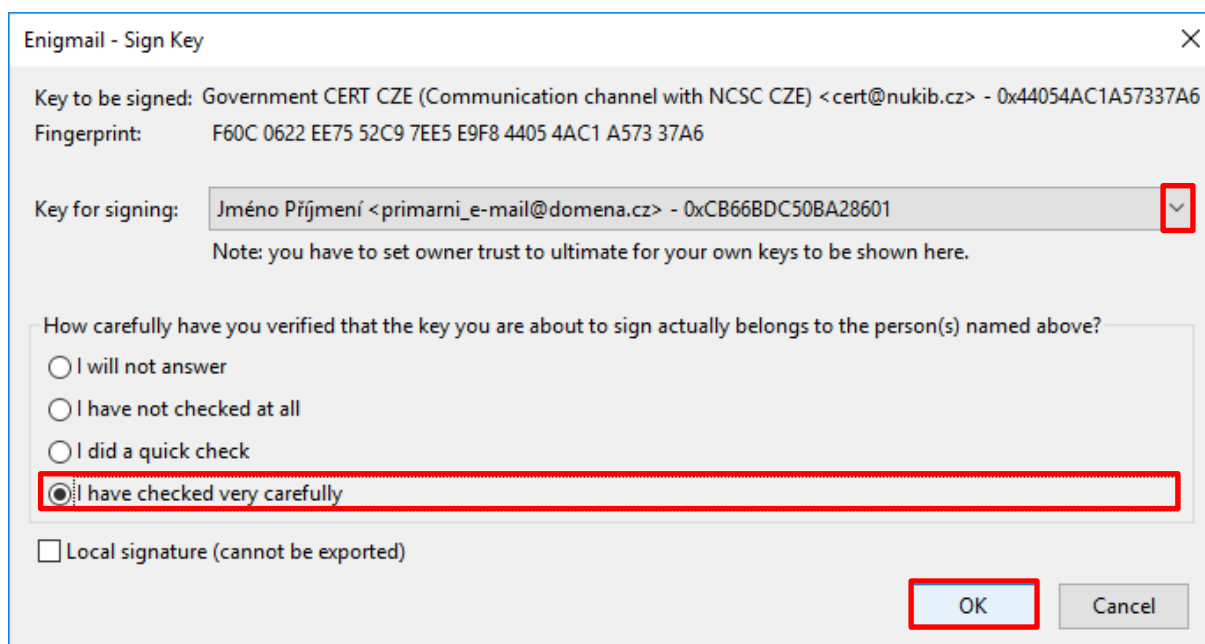




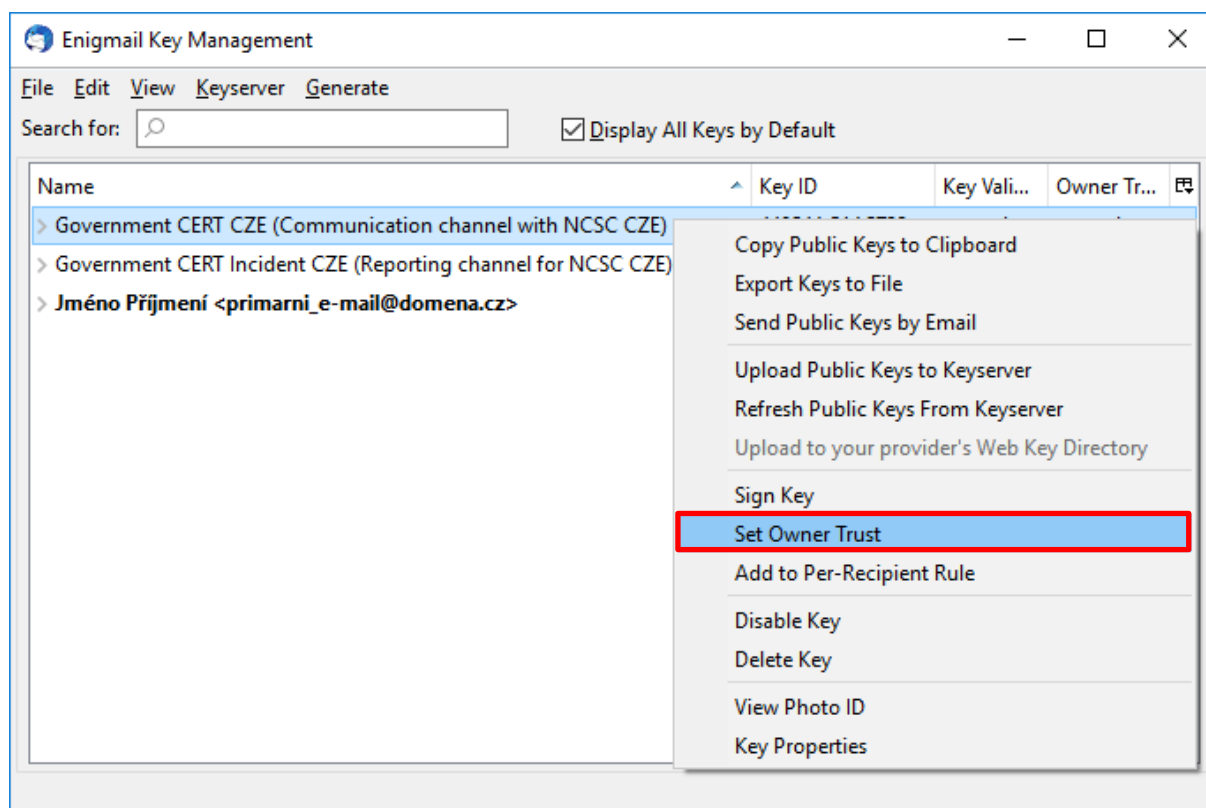
Po naimportování potřebných klíčů příjemců je potřeba tyto klíče nejprve podepsat a nastavit jejich důvěryhodnost. To se udělá následovně: pravým tlačítkem myši vyberte příslušný PGP klíč a zvolte možnost „Sign Key“ (Podepsat klíč).



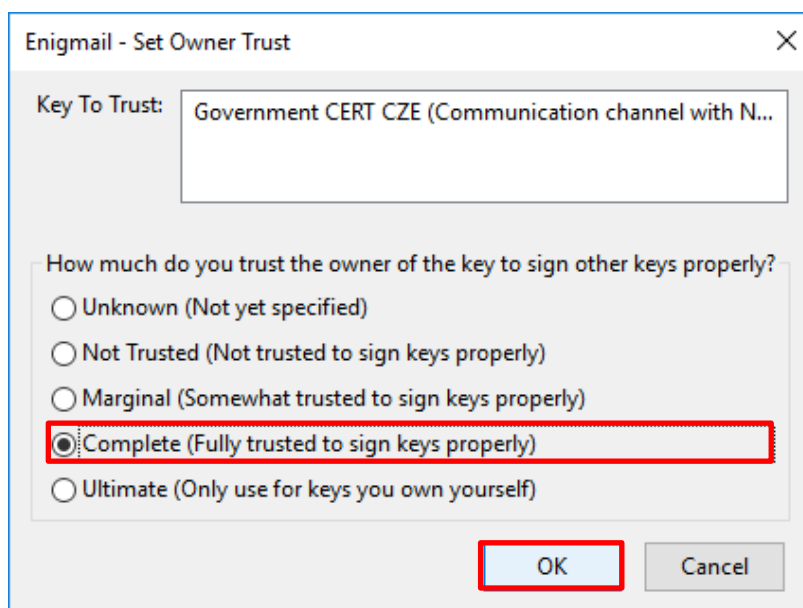
Vyberte svůj vlastní klíč, kterým budete vybraný klíč příjemce podepisovat a zvolte míru Vašeho ověření, že daný klíč patří vlastníku - v tomto případě vládnímu CERT týmu.



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).

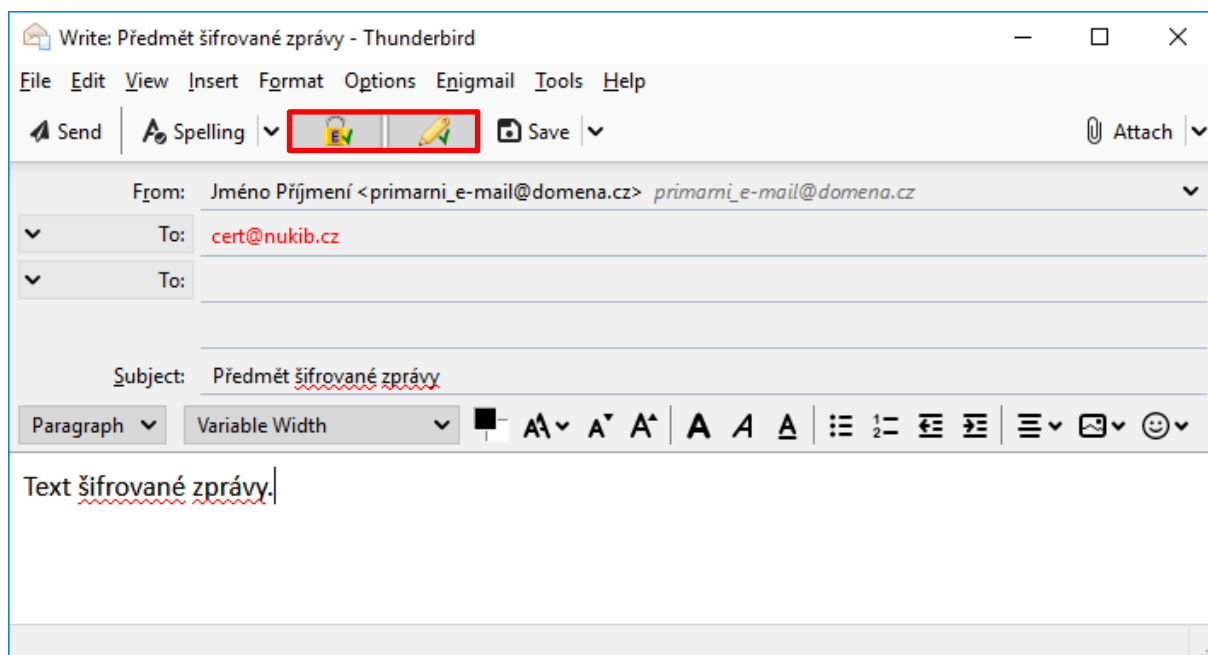


Hodnotu u klíče příjemce nastavíte dle jeho důvěryhodnosti. V případě klíčů vládního CERT týmu například nastavte „Complete“ (*Plně důvěřuji*), pokud protější straně důvěřujete. V případě vlastního klíče (odesílatele) nastavte na „Ultimate“ (*Absolutně důvěřuji*). Nyní již lze odesílat a přijímat šifrované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

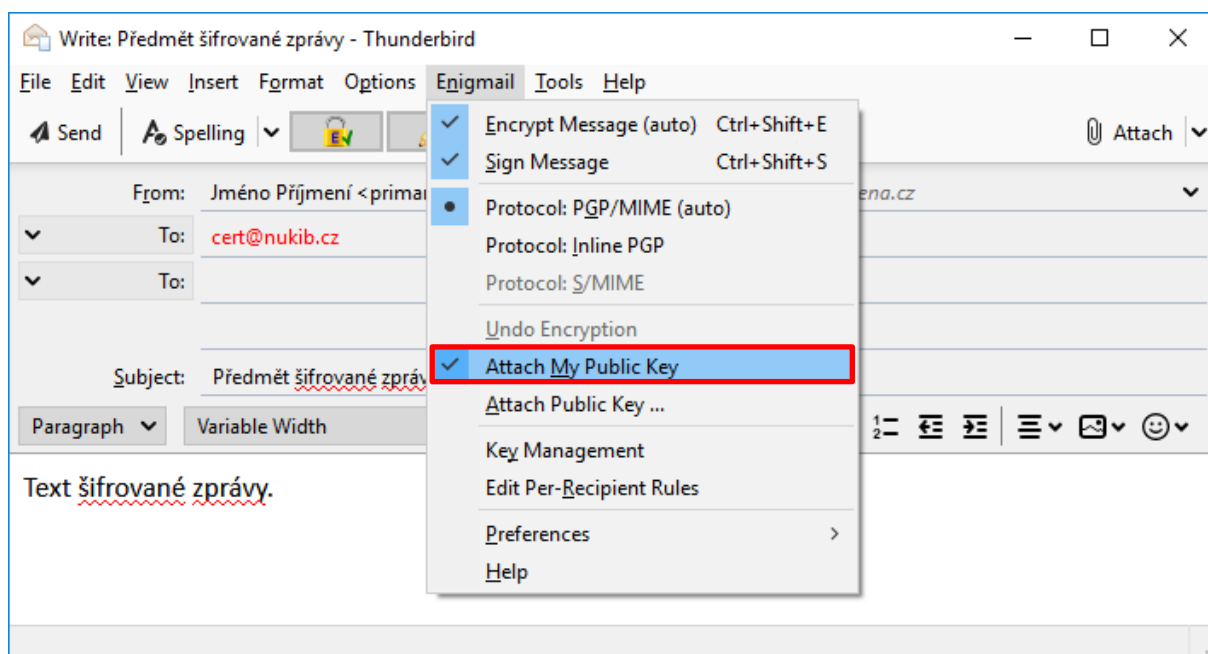


## Šifrování e-mailové zprávy

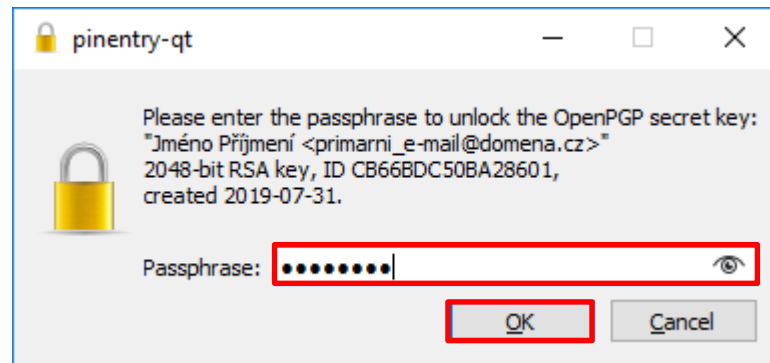
Způsob šifrování e-mailu v aplikaci Mozilla Thunderbird je následující: v hlavním menu zvolte možnost „Write“ (Napsat) a po otevření okna s novou zprávou vyplňte standardní údaje (e-mailovou adresu příjemce, předmět a tělo zprávy). E-mail následně zašifrujete kliknutím na ikonu „zámku“ a pokud chcete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



Pro obousměrnou šifrovanou komunikaci otevřete v menu zprávy položku „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 nemělo nic bránit v šifrované komunikaci mezi Vámi a Vašimi partnery.