Úvod do PGP/GPG

Aleš Padrta

PGP dle xkcd.com a xkcz.cz

Pokud si chcete být opravdu naprosto jisti, podívejte se na konec e-mailu, zda se tam nachází delší shluk podivných znaků.

Motivace

- Jsme paranoidní
  - Potřebujeme si předávat data bezpečně
- Potřebujeme
  - Šifrovat/dešifrovat
  - Podepisovat/ověřovat podpis
  - Spravovat veřejné klíče ostatních
  - Vhodný nástroj
- Existují certifikační autority … na ja, aber!
  - Nevěříme! Ověřuje někdo cizí (CIV? Terena? NSA?)
  - Věříme jen a jen sobě

PGP vs. OpenPGP vs. GNU PG

- PGP
  - Pretty Good Privacy (dost dobré soukromí)
  - Balík programů
  - Phil Zimmerman, 1991
- OpenPGP
  - Internetový standard (RFC 4880)
- GNU Privacy Guard (GPG)
  - OpenSource implementace
  - Příkazová řádka a knihovny – používáno dalšími aplikacemi

PGP/GPG je poměrně populární

Základní principy
(jak to vlastně funguje)

Klíče a jejich použití

- Každý uživatel si (sám, lokálně) vytvoří dvojici klíčů

0xA44AFFFF

Civenka.Private

Civenka.Public

Anna Nováková
civenka@civ.zcu.cz
Civenka

Jiřina.Private

Jiřina.Public

0x014104FFE

Jiřina Koťátková
jkotatko@rek.zcu.cz
Odbor Koťat

- Použití pro podpis

Zpráva od Civenky.

Civenka.Private

Zpráva od Civenky.

Civenka.Public

- Použití pro šifrování

Zpráva pro Jiřinu.

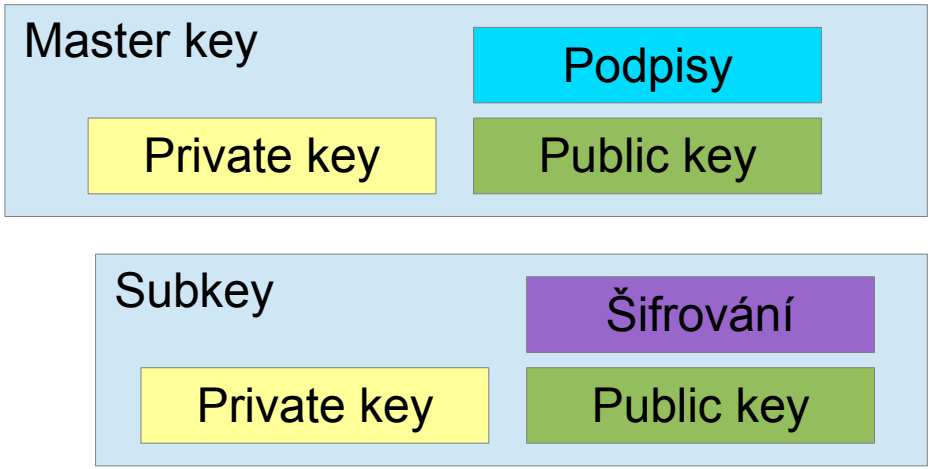
Jiřina.Public

Zpráva pro Jiřinu.

Jiřina.Private

Klíče a podklíče

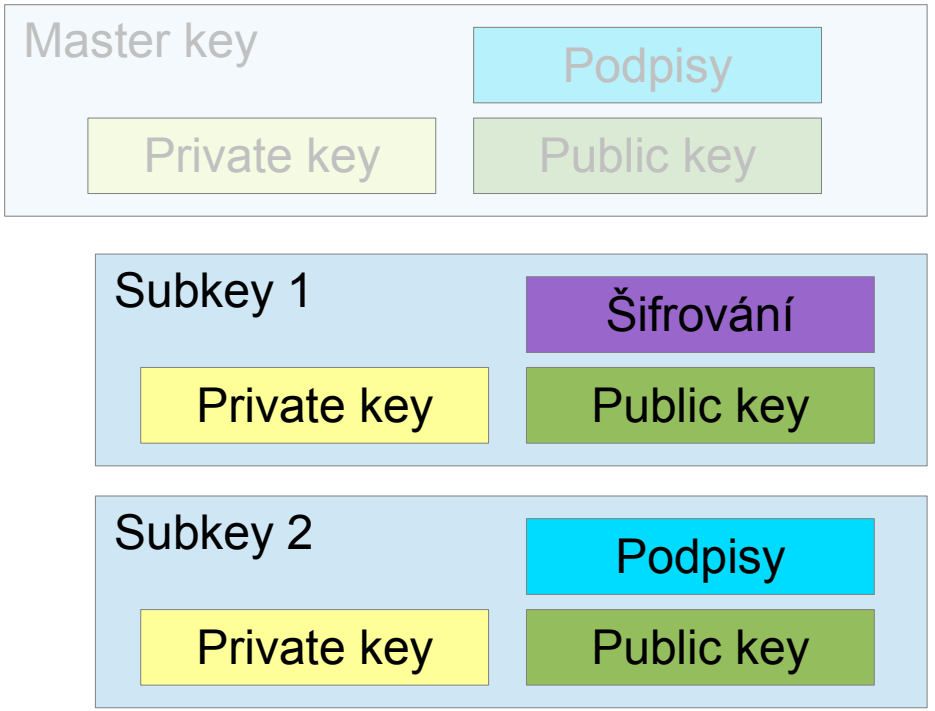
- Výchozí nastavení



- Klíč (Key) = „master key“
  - Používán k podpisu
    - Odesílané zprávy
    - Veřejné klíče
    - Svoje veřejné subklíče
  - Podepisován ostatními
- Podklíč (Subkey)
  - Používán jen k šifrování
  - Dá se vyměnit bez změny master key

Klíče a podklíče

- Hyperparanoidní

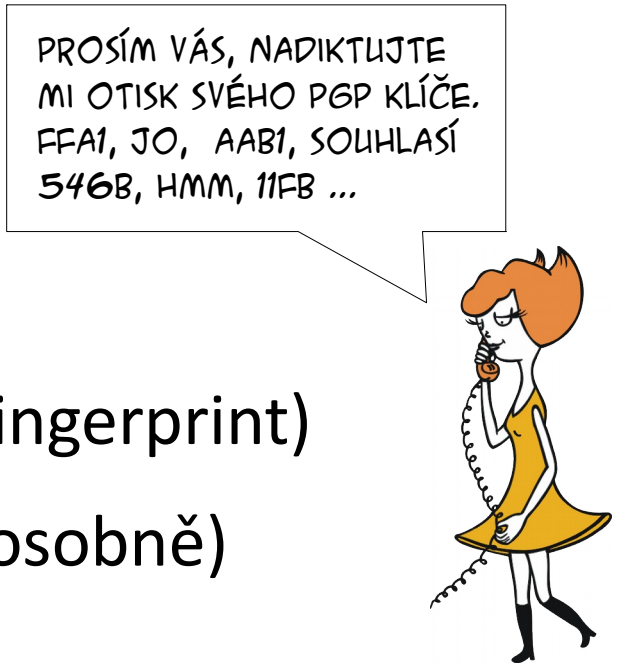


https://wiki.debian.org/Subkeys

- Klíč (Key) = „master key“
  - Uložen v „trezoru“
  - Používán pro podpis
    - Veřejné klíče
    - Svoje Veřejné podklíče
- Podklíč 1 (Subkey)
  - Používán jen k šifrování
- Podklíč 2 (Subkey)
  - Používán jen k podpisu (zprávy)

Výměna klíčů

- Musíme získat veřejný klíč druhé strany
  - Připojen ke zprávě / doručen jinak
  - Uložen ve veřejném úložiště klíčů (key-server)
- Výborně, máme veřejný klíč – jenže KOMU patří?
  - ~~Certifikační autorita by mohla …~~
  - Věříme jen sami sobě (!)
- Osobní ověření
  - Každý veřejný klíč má svůj otisk (fingerprint)
  - Kontrola jiným kanálem (ideálně osobně)



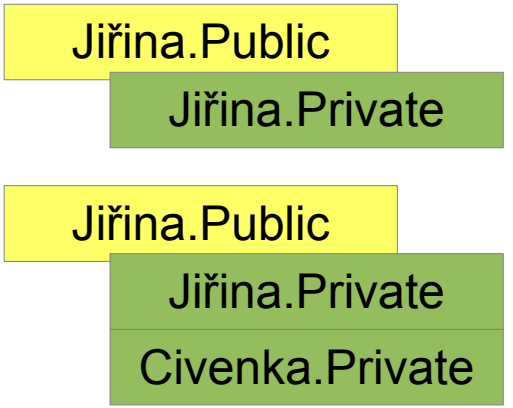
Výměna klíčů

- Zapomněnka (!)
- PGP World List
  - Pro fonetický přenos hexadecimálních čísel
  - Kódová tabulka – prodobně jako fonetická abeceda NATO (alpha, bravo, …, zulu)
  - Např. 641B E691...

    = Flytrap bravado tracker miracle …
  - https://en.wikipedia.org/wiki/PGP_word_list
  - https://warrenguy.me/projects/pgp-word-list-converter
- V praxi moc nevyužijeme

Podepisování klíčů

- Ověření fingerprintu stačí pouze 1x
- Veřejné klíče lze podepsat (pomocí master key)
  - Kdo podepsal = věří, že klíč patří uvedené osobě
  - Každý klíč je podepsán sám sebou
    - tj. autor klíče věří sám sobě :-)
  - Po ověření je klíč podepsán
    - tj. podepisovatel danému klíči věří

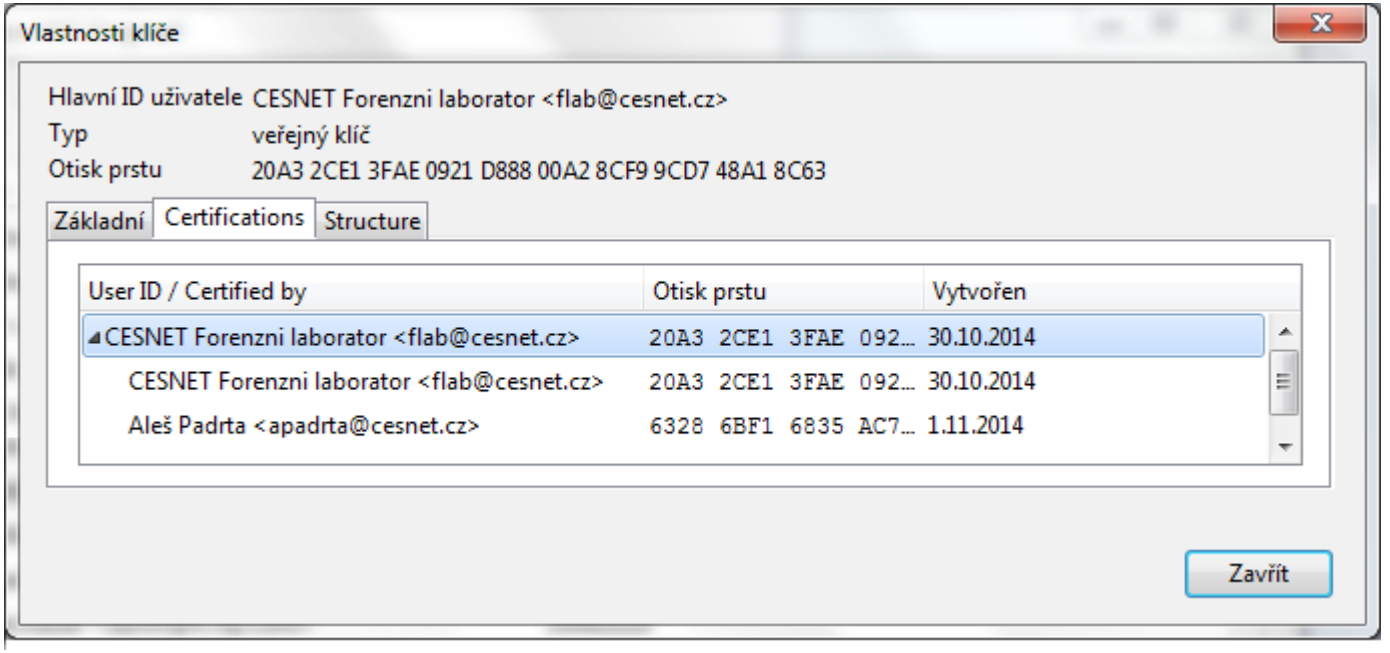


- Každý věří pouze klíčům, které sám podepsal

  = stává se certifikační autoritou (pro sebe sama)

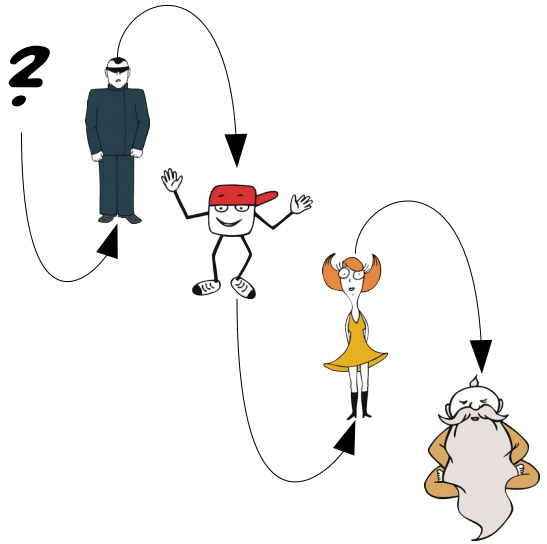
Publikování podepsaných klíčů

- Využití podepsaných klíčů
  - Lokálně (pouze pro uživatele, který podepsal)
  - Veřejně (typicky publikováno na key-servery)
- Publikované podpisy vidí i ostatní



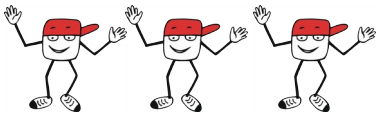
Pavučina důvěry I.

- Každý je certifikační autorita
  - Ověřuje své kontakty
  - Informace o ověřených klíčích jsou k dispozici
- Mnoho nezávislých certifikačních autorit
  - Každé lze nastavit „důvěryhodnost“
    - Nevím, neznám, nemohu říct
    - Nevěřím
    - Věřím částečně
    - Věřím plně
    - Věřím naprosto (ultimate)

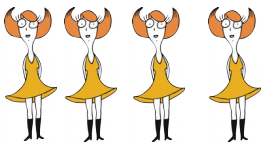
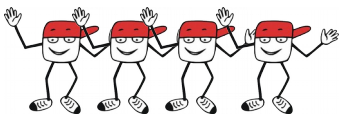


Pavučina důvěry II.

- Klasické certifikační autority
  - Hierarchický strom důvěry
- Model důvěry v PGP/GPG
  - Lze kombinovat informace od více „soukromých CA“
  - Pavučina důvěry (web of trust)
- Věříme neznámým klíčům, pokud je podepsali:

 nebo  nebo 

(v modelu důvěry „classic“, lze nastavit i jinak)

 nebo  nebo  nebo  

CA vs. PGP

- CA
  - Centrální autorita
  - Přenesení odpovědnosti za ověření
  - Hierarchický strom důvěry
- PGP
  - Individuální autorita(y)
  - Osobní ověřování a nastavení důvěry
  - Složitější pavučina důvěry

PGP lze využít pro klasickou CA

- Uživatel si podepíše klíč nově vzniklé CA
- Uživatel si nastaví pro CA úroveň „věřím plně“
- CA ověřuje a podepisuje, uživatel používá

Instalace a použití GnuPG

(praktické základy)

Instalace

- Linux
  - apt-get install gnupg

```
# apt-get install gnupg
```

- Windows
  - Gpg4win (https://www.gnupg.org/download/)
- Test správnosti

```
$ gpg --version
...
Home: ~/.gnupg
...
```

```
> gpg --version
...
Home: c:/gnupg
...
```

Konfigurace

- HOMEDIR – obsahuje „klíčenku“
  - `secring.gpg, pubring.gpg, trustdb.gpg`
- Chceme homedir na flashce
  - Jsme paranoidní – klíčenka je dostupná jen dočasně
  - Jsme pohodlní – stejná klíčenka na všech zařízeních
  - Windows
    - Systémová proměnná (cesta k umístění na USB)

```
GNUPGHOME=f:\gnupg
```

  - Linux
    - Symlink na umístění na USB

```
ln -s /media/usb0/gnupg ~/.gnupg
```

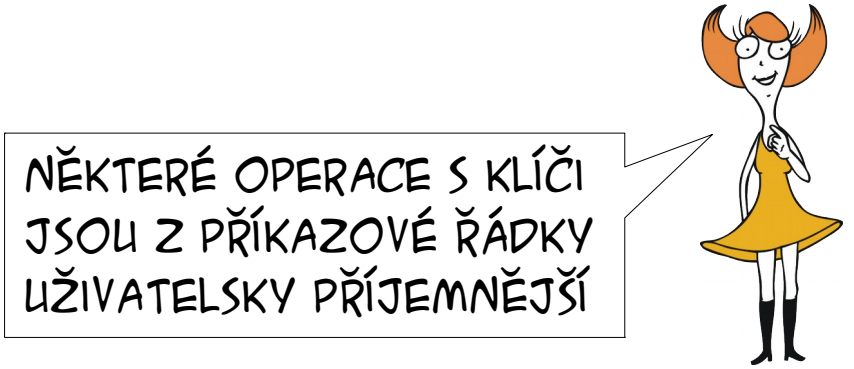
GPG z příkazové řádky

- Pro lepší pochopení + hardcore uživatele
  - Pro ostatní = GUI v SW využívajícím GPG
- Stejné pro různé OS
  - Liší se jen ve specifikaci cesty k souboru
- Základní příkazy
  - Zjištění verze a základních schopností

```
$ gpg --version
```

  - Výpis možností

```
$ gpg --help
$ man gpg      //jen linux
```



Vytvoření sady klíčů

- Spuštění

```
$ gpg --gen-key
```

- Zadávané parametry
  - Typ: RSA a RSA (default)
  - Délka klíče: 4096 (maximum – jsme přeci paranoidní)
  - Expirace: žádná (v případě potřeby použijeme revokaci)
  - Jméno: Meda Beda
  - E-mail: medabeda@civ.zcu.cz
  - Komentář: Testovaci uzivatel pro prezentaci o PGP
  - Passphrase: heslo k přístupu k privátnímu klíči

Kontrola klíčů v klíčence

- Veřejné klíče

```
> gpg --list-keys
F:/gnupg/pubring.gpg
------------------------------------------------

pub   4096R/0DFE1634 2016-04-14
uid   [  absolutní ] Meda Beda (Testovaci uzivatel pro prez
entaci o PGP) <medabeda@civ.zcu.cz>
sub   4096R/7B381829 2016-04-14
```

- Privátní klíče

```
> gpg --list-secret-keys
F:/gnupg/secring.gpg
------------------------------------------------

pub   4096R/0DFE1634 2016-04-14
uid   [  absolutní ] Meda Beda (Testovaci uzivatel pro prez
entaci o PGP) <medabeda@civ.zcu.cz>
sub   4096R/7B381829 2016-04-14
```

Revokace klíčů

- Pro případ kompromitace klíče

```
$ gpg --output revoke.asc --gen-revoke 0DFE1634   //"podepisovací" klíč
$ gpg --output revoke.asc --gen-revoke 7B381829   //"šifrovací" podklíč
```

- Zadávané údaje
  - Důvod revokace: Kompromitován/zrušen/nahrazen
  - Popis: možno podrobněji popsat důvod
  - Passphrase: (k odemčení privátního klíče)
- Výstup
  - Soubor `revoke.asc`
  - Doručit druhé straně (key-server)

```
$ cat revoke.asc

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2
Comment: A revocation certificate should follow

iQIfBCABCAAJBQJXFJKXAh0AAAoJEJsZ89IN/hY0VQgP/jmoWzFmLAweqiVEWaMX
un4QmzowwxocGgCLq5HWun8hxMAQGp6pvDnmI4Yqo5uA8WJyCy8pNHriFP9XQpGz
/6eHNEXz6H7G1VRRL1R0fSFEBnrFnu3mQXbh9/jH8TQpm1ZcZzsCB5KxqmTdpvSq
LBJcqmFDFHevfyYveAA3ToIWo0gmGe0/URQ+A4jfRwohoj89URPGSNORW7Xmgsx1
l1vhrZ4+DzWKObFNM/RVJ8IqmEA7DyudOovUL3tEOpRcALz9WNPfstmRqyDlurE2
zPBxm9ZzPrLu4HWKmCrtBcqsq+fsMArCtE/nhY+GtSXrMXG94RYYSRZTdNkfqWiu
fmqwx5+m+lLDp4bn6Dk8t6RbTUmyTDf6BHBCdwr1PEtIgkjBf6ZF4Spu02RLrla8
SR0yWoY0xFi68e8ADhSqdgEnibdBhPQa14Gu5+pXRgxpCH5pnZyDuDTcFBjI1eU4
TSmjA7smoFiohW6sqATRgUxIQGoHBtu0AAl1OQmbBgKeGEhRZ8TOuZRfHg8IhqC3
30a70zMG3KqULNdDB7pWCURlS/Uv4z6DBI7GxEmWujyIkpwPWXBQT55gSkxHiLso
FuOG+bLcx7jiXn0VTD9XErYs8Mcd6aAT579EFvViwJ/W0FPWnNJmVrlKwlTW2S9t
IQWwueq+BdYdUAh7RjLJPaH5
=Hpd2
-----END PGP PUBLIC KEY BLOCK-----
```

Výměna veřejných klíčů

- Ručně
  - Export veřejných klíčů – včetně jejich dalších podpisů

```
$ gpg --output pubkeys.all --export                    //všechny
$ gpg --output pubkey.7a2232a8 --export 7A2232A8       //specifikovaný
```

  - Import veřejných klíčů (druhá strana komunikace)

```
$ gpg --import pubkeys.all
$ gpg --import pubkey.7a2232a8
```

- S pomocí key-serverů

```
$ gpg --send-keys --keyserver wwwkeys.cz.pgp.net 7A2232A8
```

```
$ gpg --recv-keys --keyserver wwwkeys.cz.pgp.net 7A2232A8
```

```
$ gpg --search-keys --keyserver wwwkeys.cz.pgp.net civenka
```

```
$ gpg --refresh-keys --keyserver wwwkeys.cz.pgp.net
```

Podepisování klíčů I.

- Máme veřejný klíč, co s tím?
- Nejdřív ověřit!

```
$ gpg --fingerprint 48A18C63
pub   2048R/48A18C63 2014-10-30
  Otisk klíče = 20A3 2CE1 3FAE 0921 D888  00A2 8CF9 9CD7 48A1 8C63
uid   [nedefinovaná] CESNET Forenzni laborator <flab@cesnet.cz>
sub   2048R/5DCCC3C7 2014-10-30
```

- Zjistit jaký fingerprint má (u sebe) druhá strana
  - Osobní návštěva
  - Telefonát na známé číslo (známý hlas)
  - PGP párty (seznámení, ověření)

Podepisování klíčů II.

- Ověřený klíč podepíšeme
  - Tím je „pro nás“ ověřený/důvěryhodný

```
$ gpg --edit-key -u <kdo podepisuje> <co je podepisováno>
$ gpg --edit-key -u 0DFE1634 48A18C63
gpg> sign
```

- Postup
  - Prohlédnout si informace (klíč, fingerprint)
  - Potvrdit podpis
  - Zadat passfrázi (k privátnímu klíči podepisovatele)
- Upload – využití ostatními / jinde

```
$ gpg --send-keys --keyserver wwwkeys.cz.pgp.net 48A18C63
```

Nastavení důvěry

- Nechť je naše paranoia limitována
  - Věříme, že FLAB umí ověřovat (čistě hypoteticky!)
  - Nastavení důvěry pro klíč FLAB

```
$ gpg --edit-key -u <kdo nastavuje> <co je nastavováno>
$ gpg --edit-key -u 0DFE1634 48A18C63
gpg> trust
```

  - Nastavení úrovně: plně důvěřuji
  - Přepočítání pavučiny (pro aktuálně importované klíče)

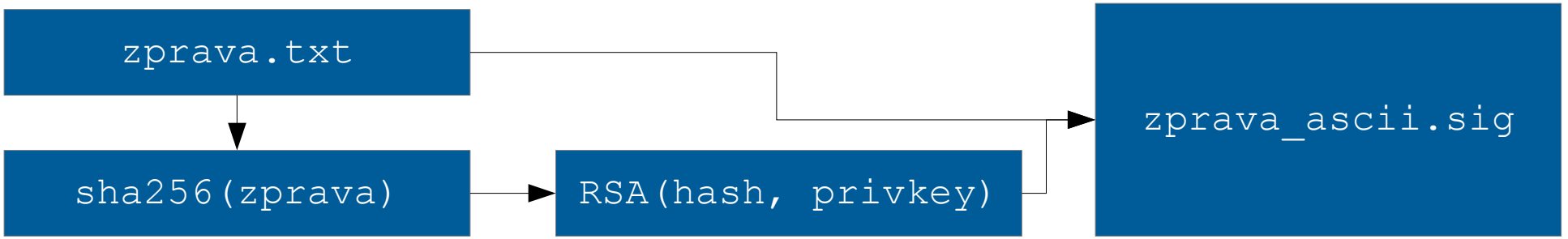
```
$ gpg --check-trustdb
```

- Dávkové nastavení pro všechny klíče (inicializace)

```
$ gpg --update-trustdb
```

Digitální podpis

```
$ gpg --output zprava_ascii.sig --clearsign --sign zprava.txt
```



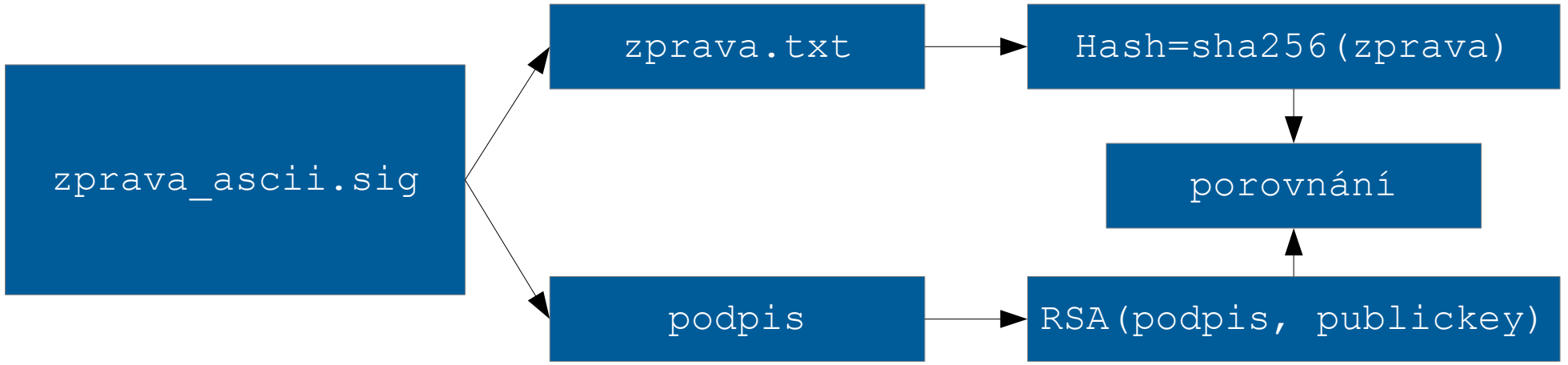

```
cat zprava_ascii.sig
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

"Podepsana zprava od Medi Bedi"
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iQIcBAEBCAAGBQJXFOuGAAoJEJsZ89IN/hY0qc8QAJIUtwK1wO8Y3zXmrdJTEw3+
...
vqLF604pHYgkTnuARPWVCnTabN70LqyaqlbO/3whLZ1OEpXDUXIzPhUncqYBn1Rz
M9jOuPlzKKjq5d15xteP
=zn4y
-----END PGP SIGNATURE-----
```

Ověření digitálního podpisu

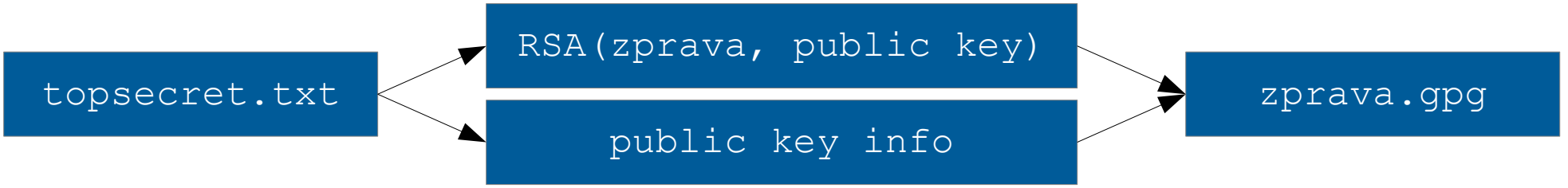
```
$ gpg --verify zprava_ascii.sig
gpg: Podpis vytvořen 04/18/16 14:47:01 Střední Evropa (letní čas) pomocí
     klíče DSA s ID uživatele 0DFE1634
gpg: Dobrý podpis od „Meda Beda (Testovaci uzivatel pro prezentaci o PGP)
     <medabeda@civ.zcu.cz>“ [absolutní]
```




```
$ gpg --verify zmenena_zprava_ascii.sig
gpg: Podpis vytvořen 04/18/16 14:47:01 Střední Evropa (letní čas) pomocí
     klíče DSA s ID uživatele 0DFE1634
gpg: ŠPATNÝ podpis od „Meda Beda (Testovaci uzivatel pro prezentaci o PGP)
     <medabeda@civ.zcu.cz>“ [absolutní]
```

Zašifrování souboru

```
$ gpg --output zprava.gpg --encrypt --armor --recipient civenka topsecret.txt
```



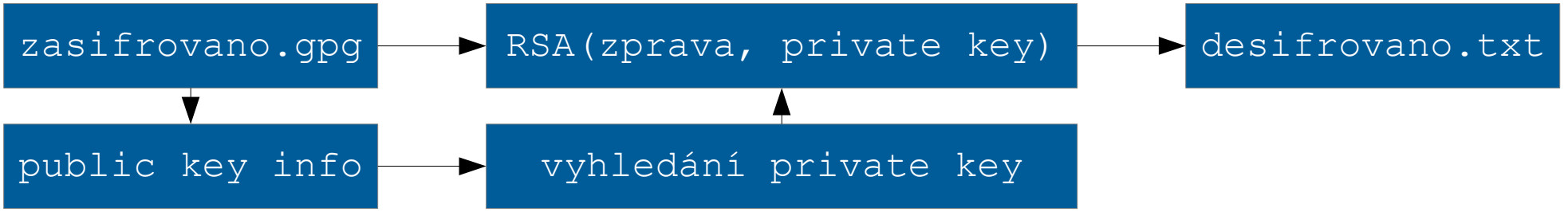

```
cat zprava.gpg

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.12 (GNU/Linux)

hQIMAyUTI2rhlT7yAQ//VmiuGO+l9k662RUd6gVZQ2TLJUK6xQtUGi2BGhtXVhUv
+OMG91C/9FQOfda/s00+WASNP1zO5VT/LjJH75KkPTfkvfVTI3w+efgEhHNpcXcj
...
ZgGq/8I79ySFIdBR+cn1T7n2YqtMCLm+H6hapCS6rBFbF1Hik0BXxSjjhCXQSpxA
gq00SrUX2DUju89jtPnnhWIsi8VrRL5hvU/skOfD+yfmg+qaKXunk7FcL+YZbAoA
MuwbrwxpRQ==
=r8Hr
-----END PGP MESSAGE-----
```

Dešifrování souboru

```
$ gpg --output desifrovano.txt --decrypt zasifrovano.gpg
```



- Výsledek se správným klíčem (otevírá Civenka)

```
cat desifrovano.txt

hypertajna zprava pro civenku
```

- Bez správného klíče (otevírá někdo jiný)

```
gpg: zašifrována 4096-bitovým RSA klíčem, ID E1953EF2,
     vytvořeným 2015-06-26 "Anna Nováková (Civenka)
     <civenka@civ.zcu.cz>"
gpg: dešifrování selhalo: tajný klíč není dostupný
```

Podpis a šifrování současně

- Podpis a zašifrování (výstup v ASCII)

```
$ gpg --output encrypted-signed.gpg --armor --recipient civenka
   --encrypt --sign topsecret.txt
```

- Dešifrování a ověření podpisu (současně)

```
$ gpg --output desifrovano.txt --decrypt encrypted-signed.gpg
gpg: Podpis vytvořen 04/18/16 14:47:01 Střední Evropa (letní čas) pomocí
     klíče DSA s ID uživatele 0DFE1634
gpg: Dobrý podpis od „Meda Beda (Testovaci uzivatel pro prezentaci o PGP)
     <medabeda@civ.zcu.cz>“ [absolutní]
```

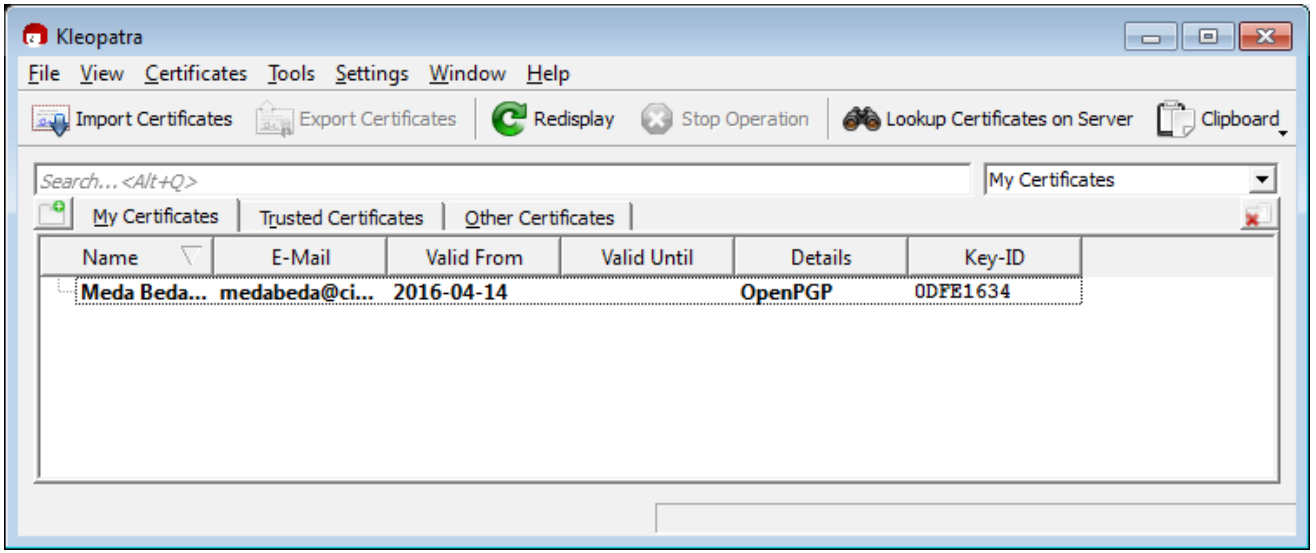
```
$ cat desifrovano.txt
Hypertajna zprava pro civenku od Medi Bedi.
```

Zajímavosti a nástrahy

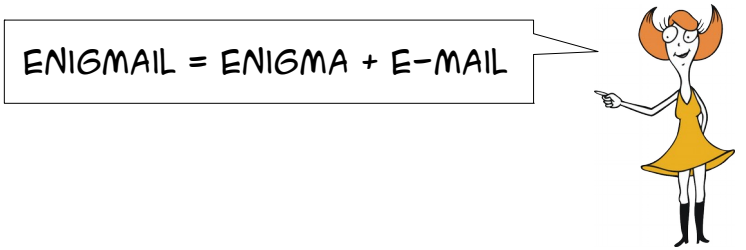
- Pořadí parametrů (nastavení)
  - Některé nelze prohodit (na pořadí záleží)
- Specifikace pro uložení výstupu
  - Přepínač `--output`
- Přinucení k ASCII (base64) výstupu
  - Přepínače `--clearsign` a `--armor`
- Pokud existuje máme více indentit (privátních klíčů)
  - Přepínač `-u` nebo `--local-user <specifikace klíče>`
- Vyhledání/specifikaci klíče
  - ID, jméno uživatele, e-mail … nebo jejich části

Používání GnuPG

- Příkazová řádka
- Speciální nástroje s GUI
  - Kleopatra - lze instalovat v rámci Ggp4win



- Aplikace využívající knihoven GnuPG
  - Mozilla Thundebird, MS Outlook, Jabber, ...

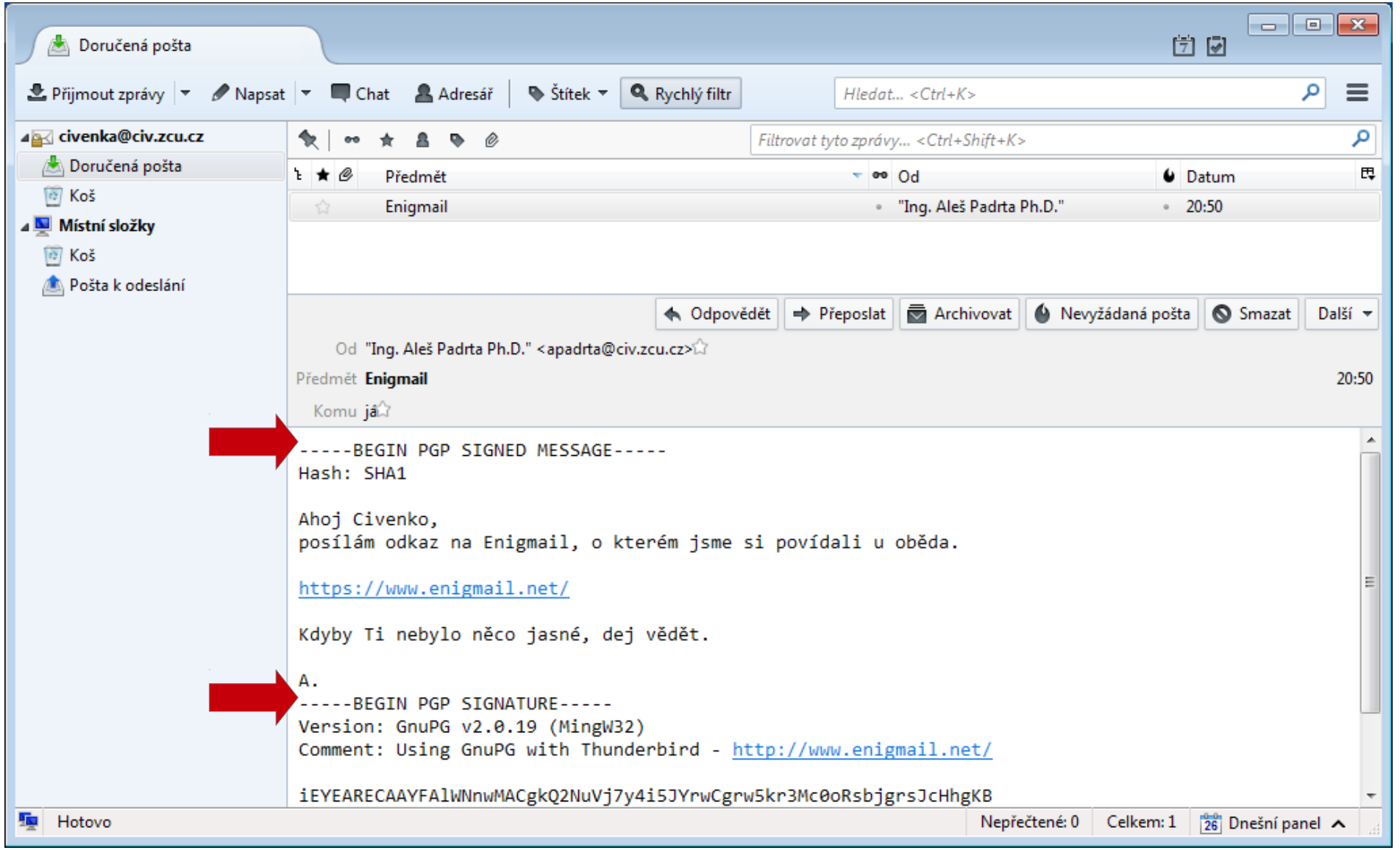


GPG a Mozilla Thunderbird

(rozšíření Enigmail)

Civenka se setkává s PGP

E-mail podepsaný PGP



Už bychom uměli ověřit

- Označit vše mezi

```
-----BEGIN PGP SIGNED MESSAGE-----
...
-----END PGP SIGNATURE-----
```

- Zkopírovat a uložit do souboru zprava.txt

```
$ gpg --verify zprava.txt
gpg: Podpis vytvořen 04/18/16 20:50:02 Střední Evropa (letní čas)
     pomocí klíče DSA s ID uživatele BCB88B92
gpg: Dobrý podpis od „Aleš Padrta <apadrta@cesnet.cz>"
gpg:                 alias „Ales Padrta <apadrta@civ.zcu.cz>"
```

- Nepohodlné
  - Naučíme Thunderbird, aby to umět zařídit

Enigmail

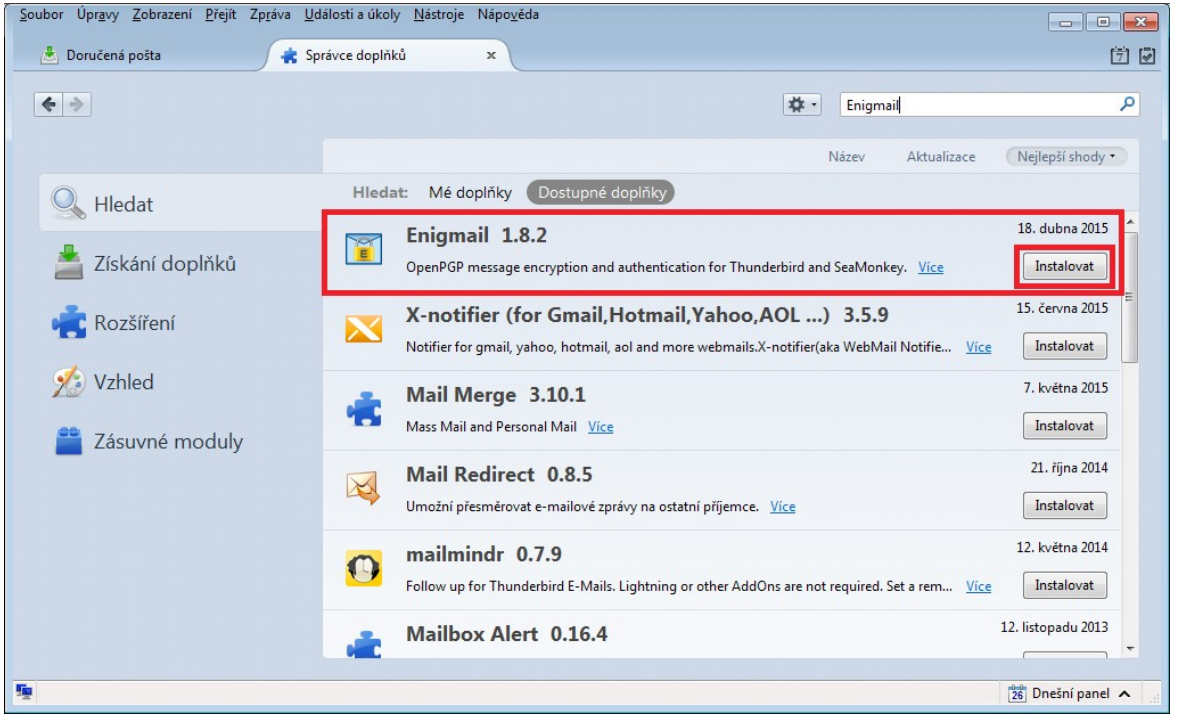
- Rozšíření pro Mozillu Thunderbird
  - OpenSource
- Využívá GnuPG
  - Šifrování
  - Digitální podpis
- Potřeba najít kompatibilní verze
  - Enigmail vs. Thunderbird
  - Obvykle obě nejnovější

Instalace

- Linux

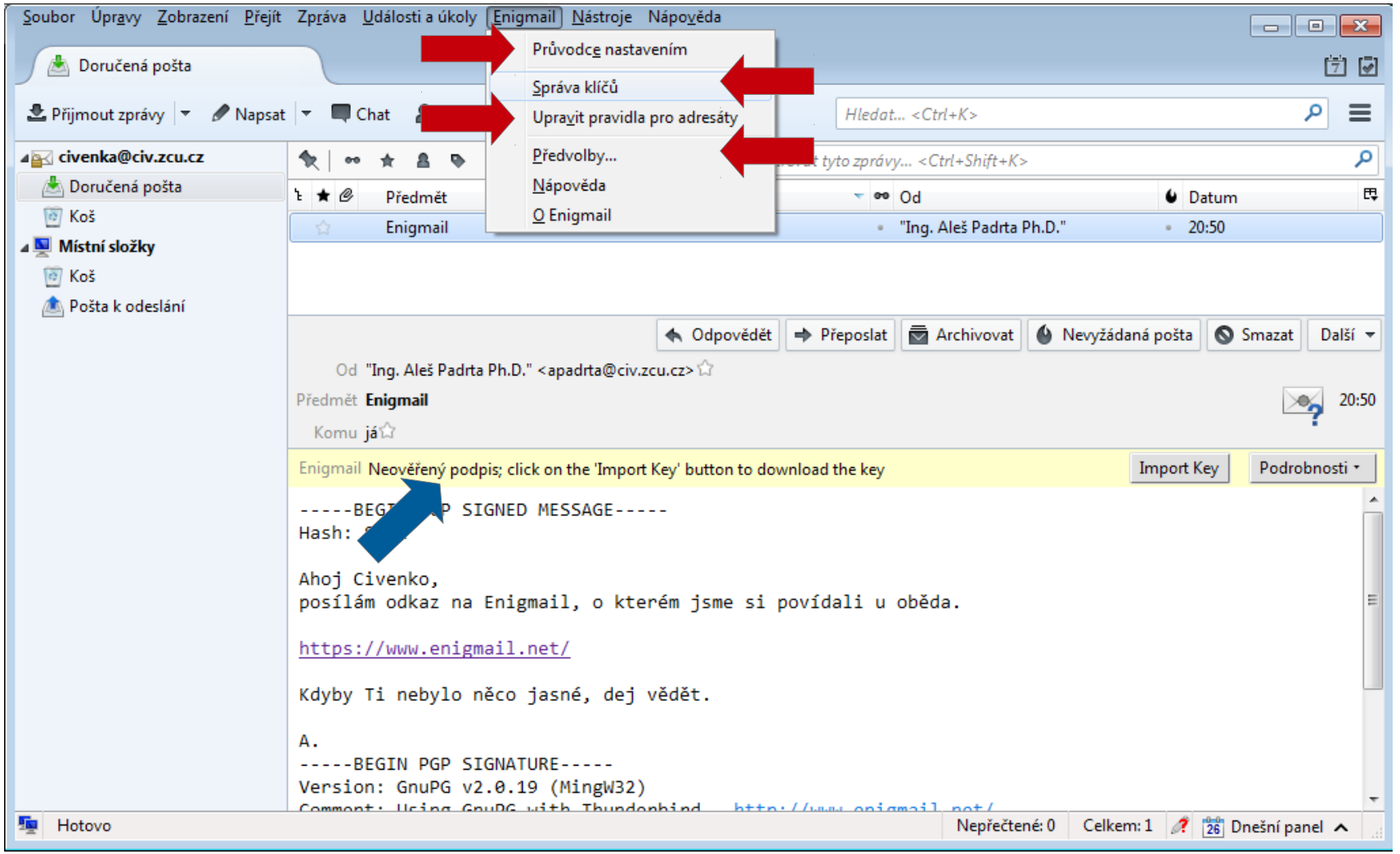
```
# apt-get install enigmail
```

- Windows
  - Správce doplňků
  - Průvodce
  - Gpg4win
  - Nabídka automatické konfigurace



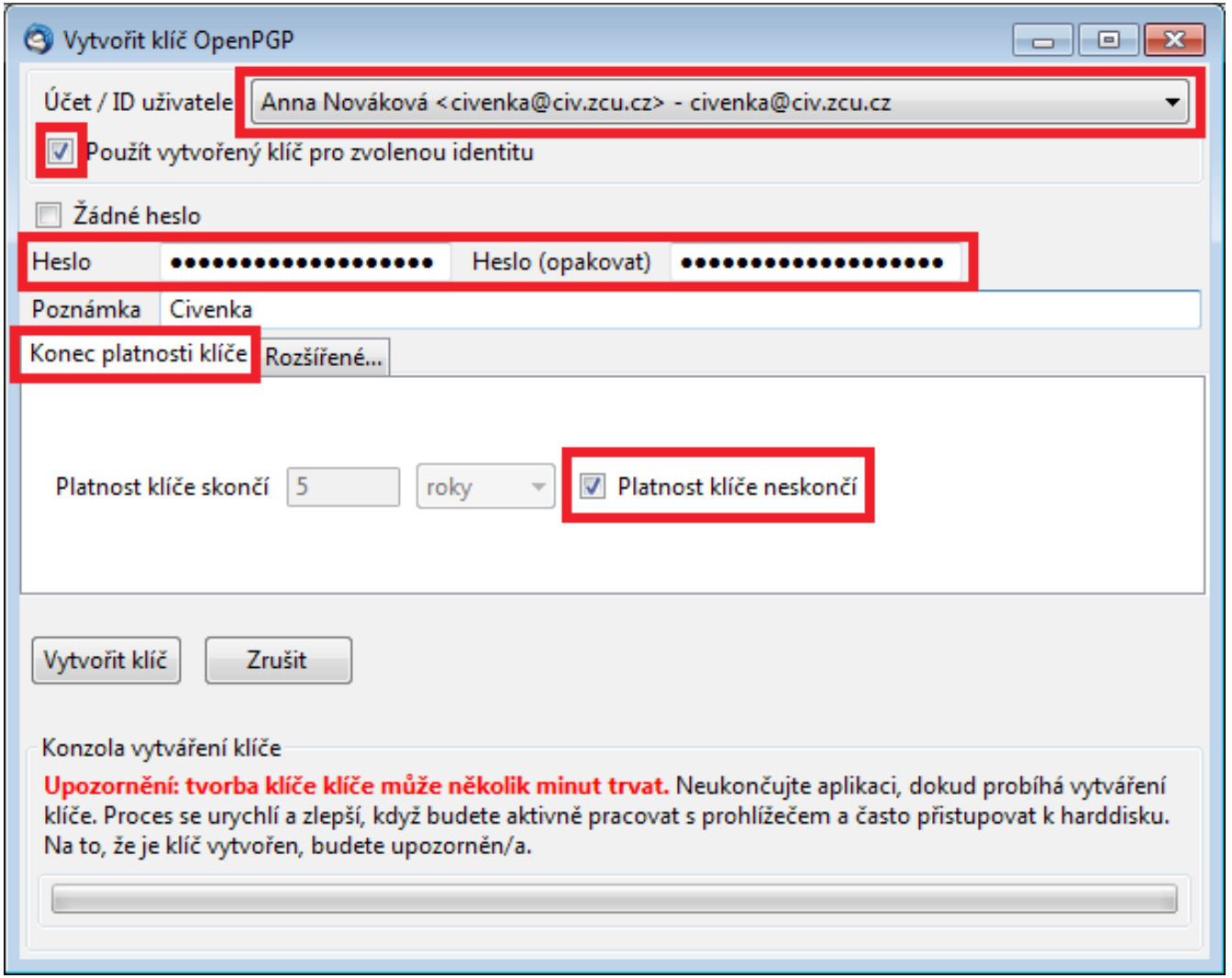
Konfigurace

- Menu „Enigmail“



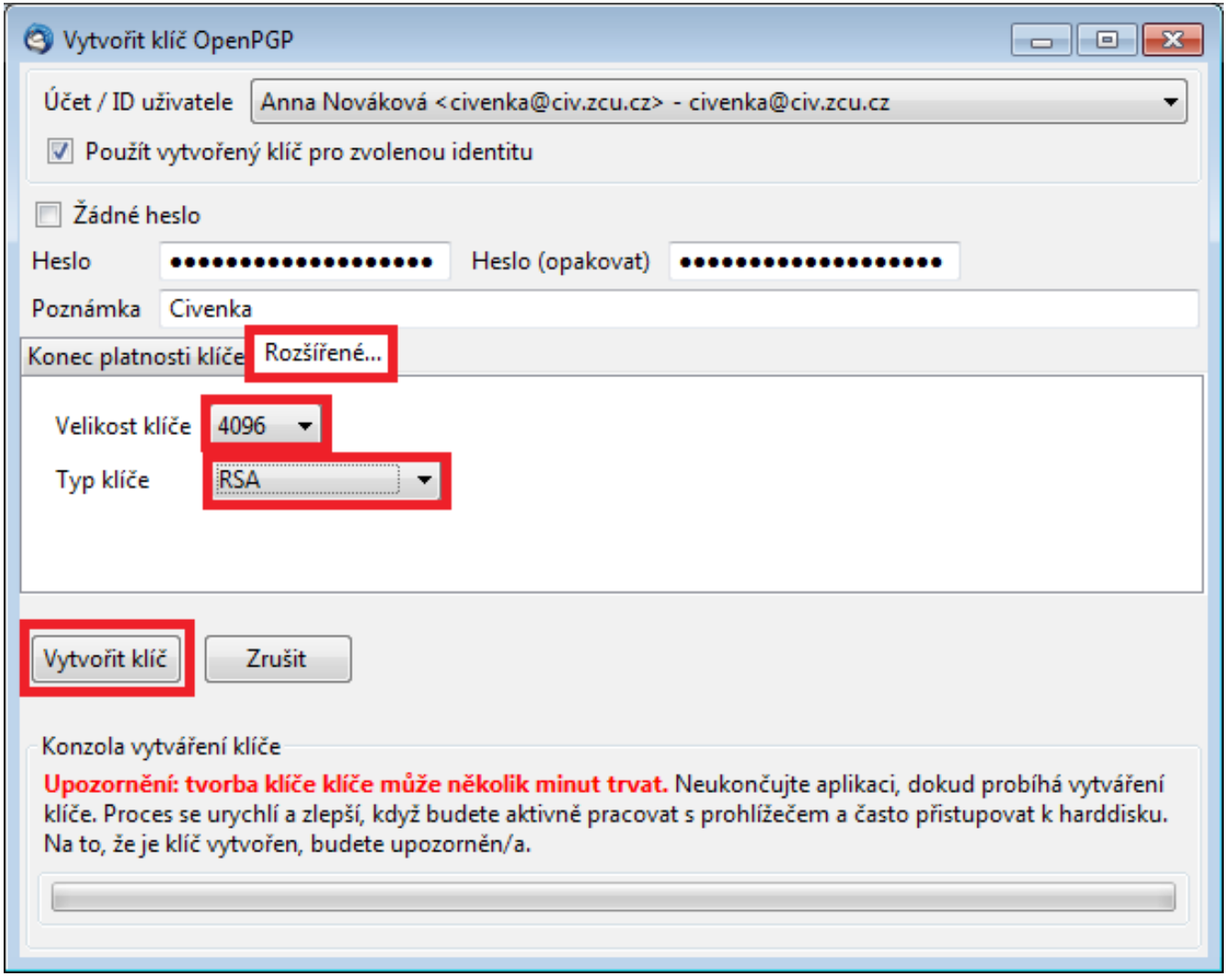
Vytvoření nových klíčů

- Enigmail > Správa klíčů > Nový pár klíčů



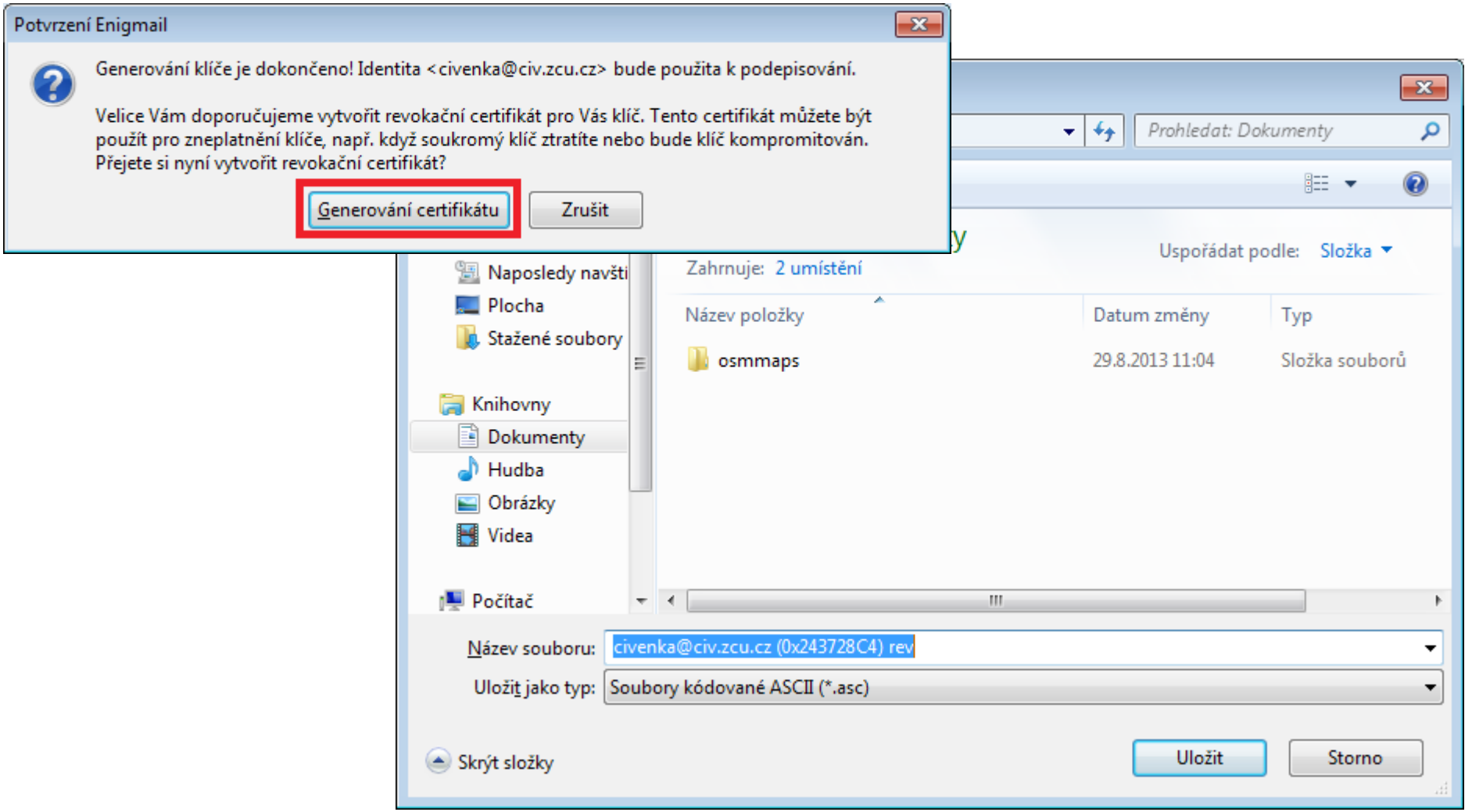
Vytvoření nových klíčů

- Enigmail > Správa klíčů > Nový pár klíčů



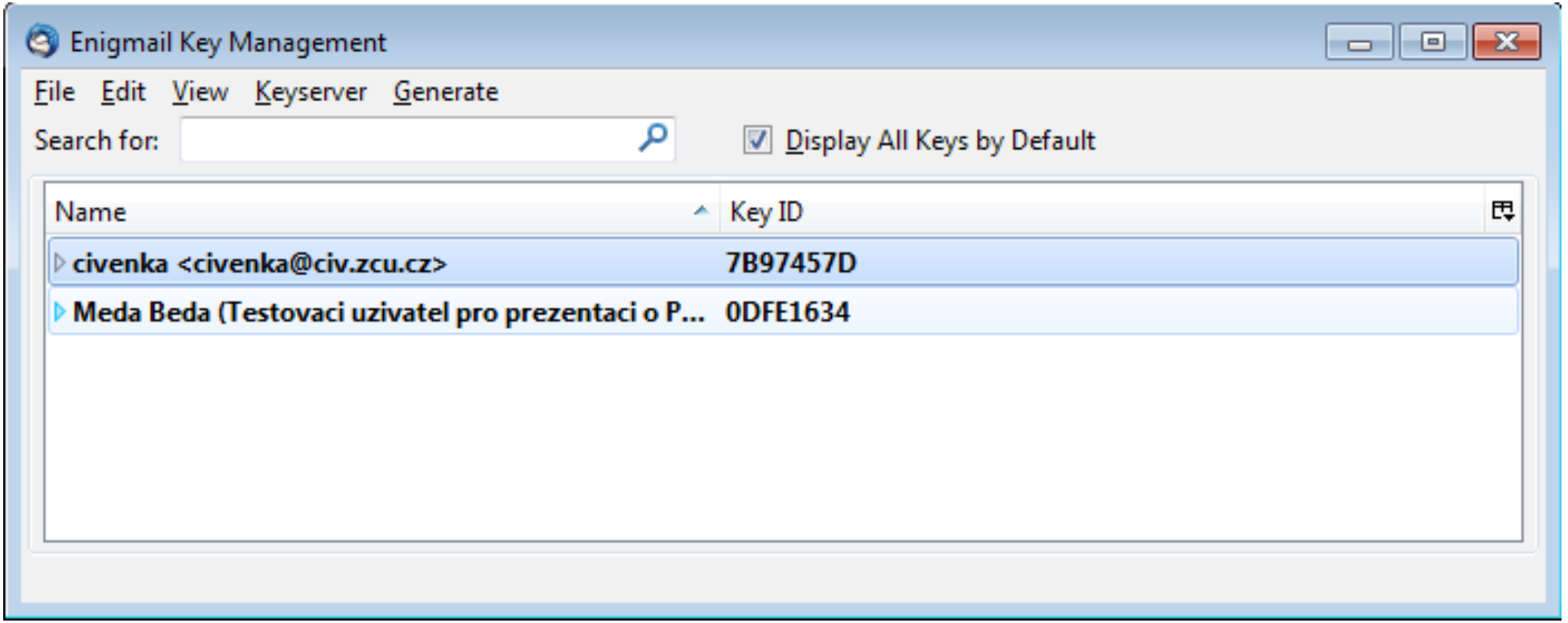
Revokační certifikát

- Automatická nabídka pro vygenerování



Přehled klíčů

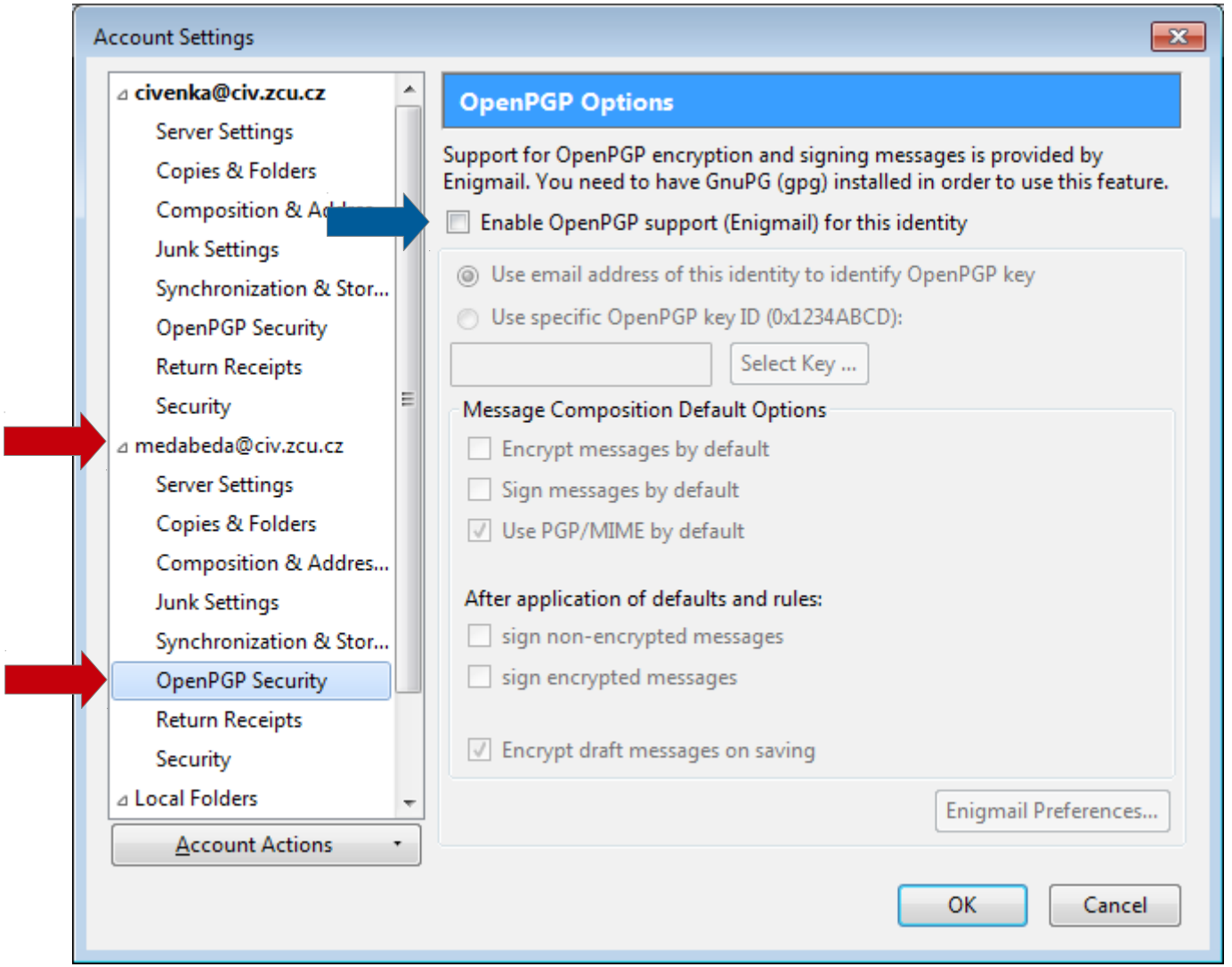
- Enigmail > Správa klíčů



- Nově přidaný klíč pro Civenku
- Testovací uživatel Méďa Béďa (už v gpg klíčence byl)

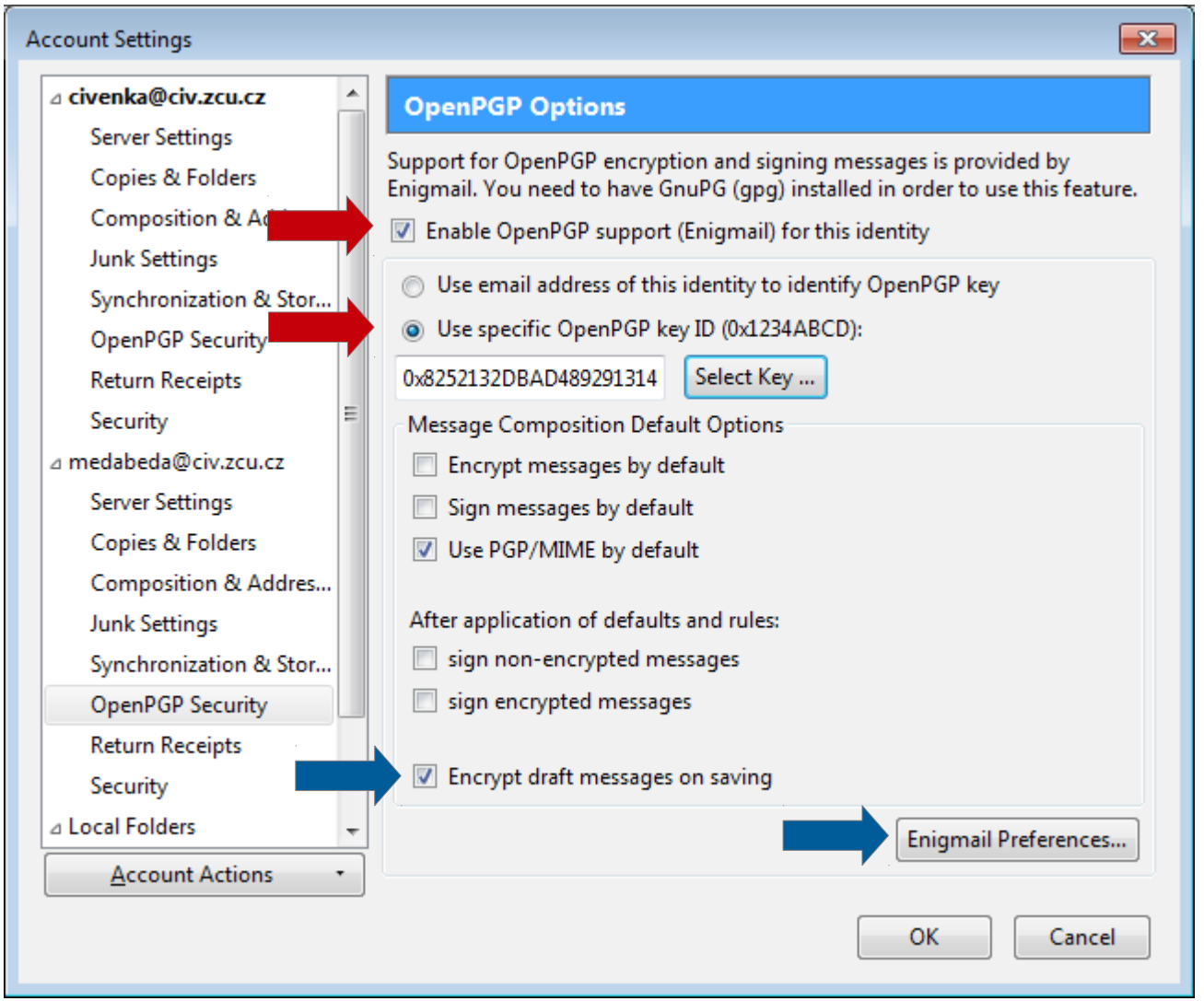
Jak přiřadit už existující klíče

- Nástroje > Nastavení účtu



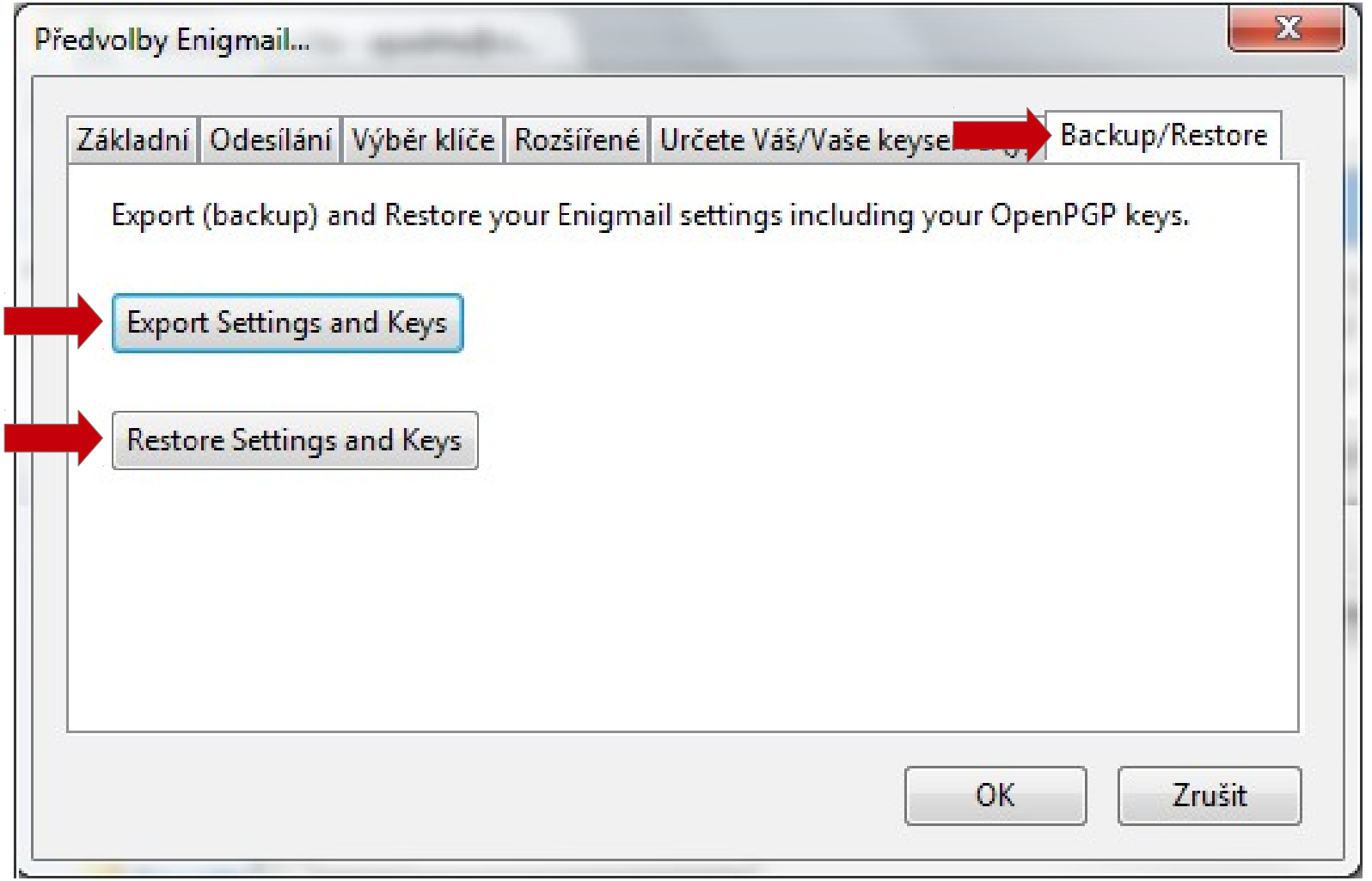
Jak přiřadit už existující klíče

- Aktivovat PGP, vybrat způsob



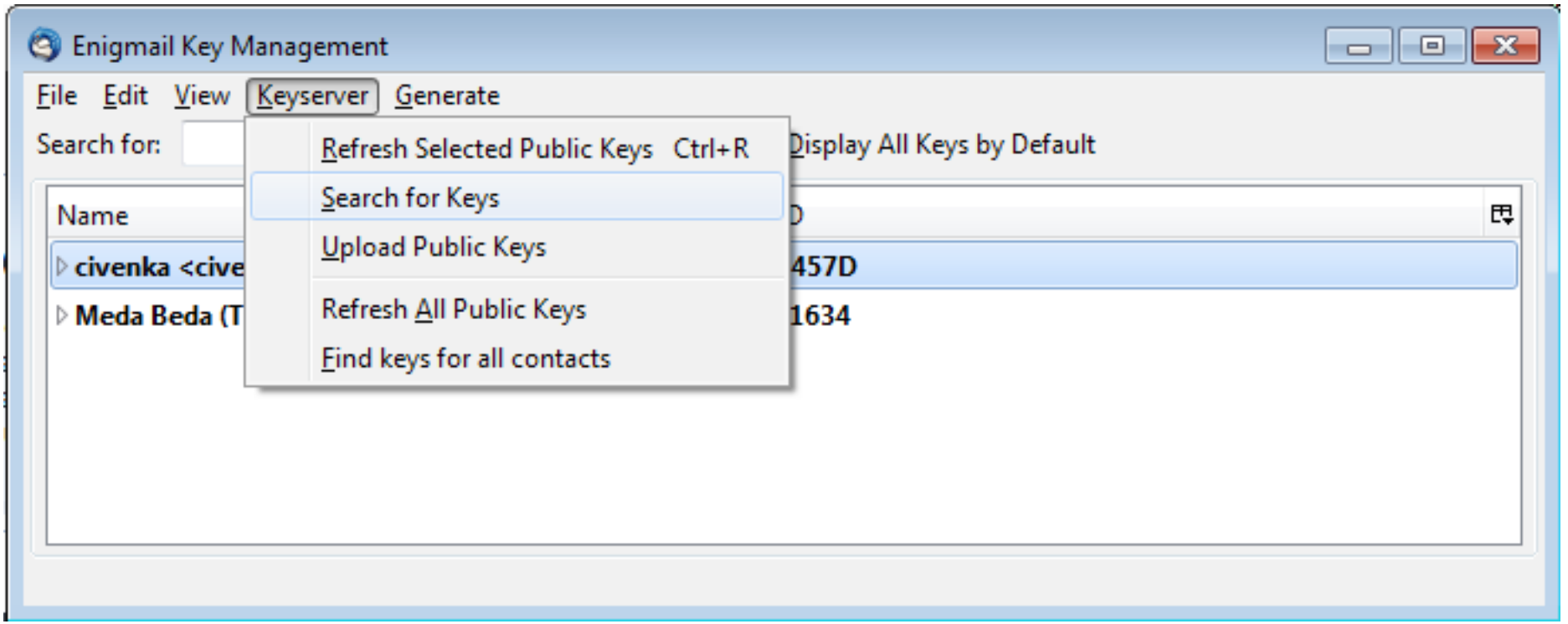
Uložení/Obnova nastavení

- Nástroje > Nastavení účtu > Enigmail Preferences

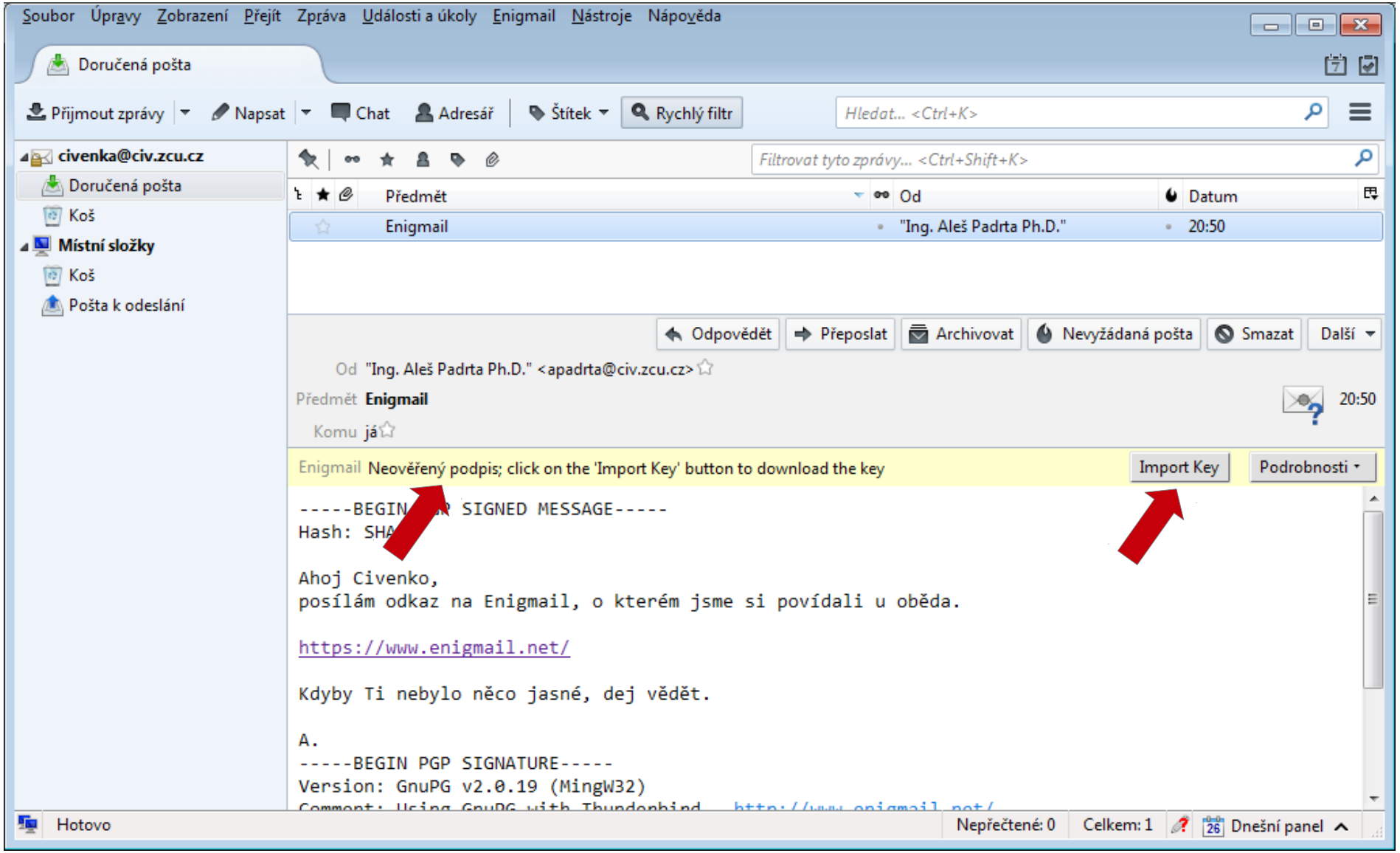


Práce s key-servery

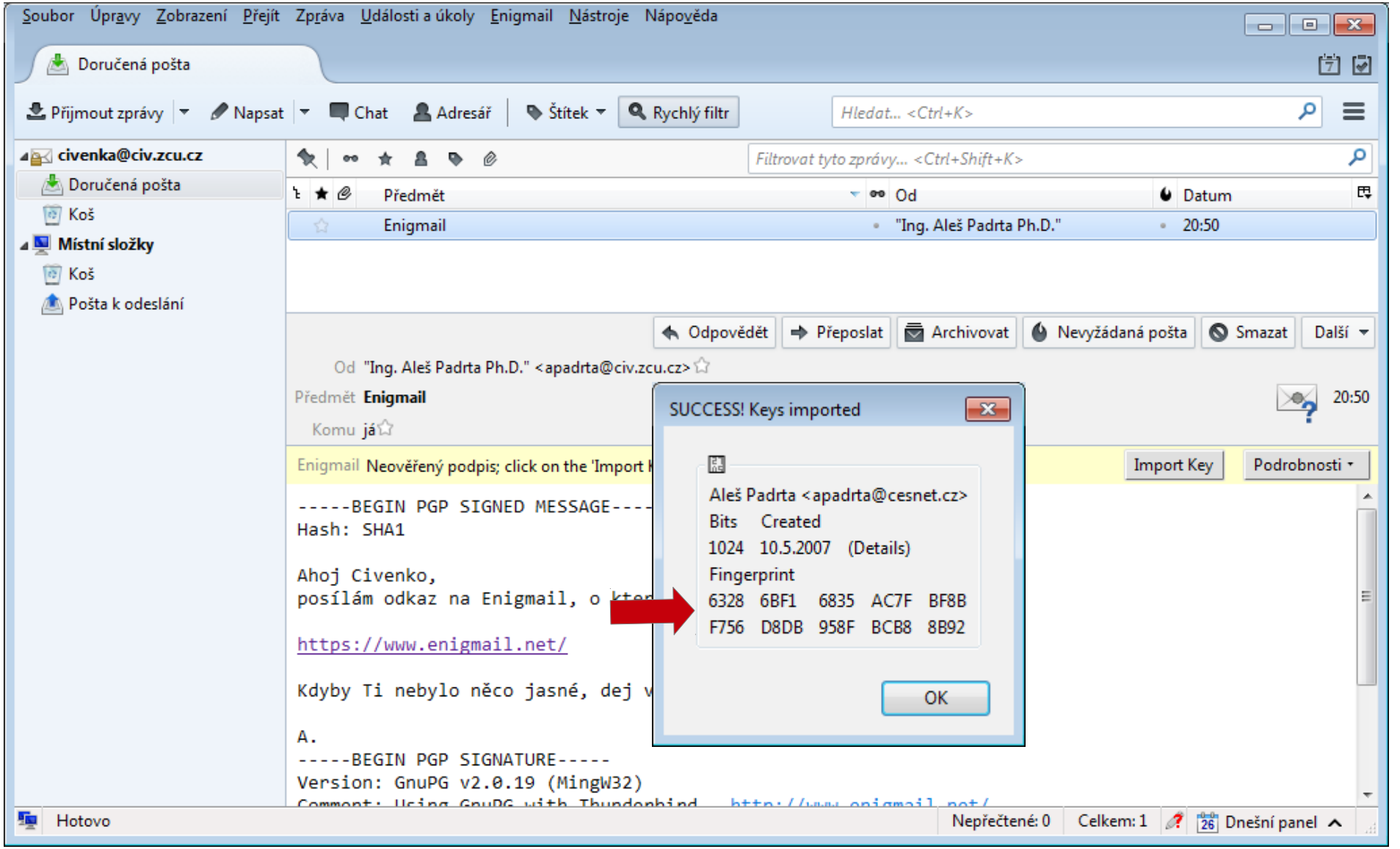
- Enigmail > Správa klíčů > Keyserver
- Vyhledání + import/export
- Aktualizace



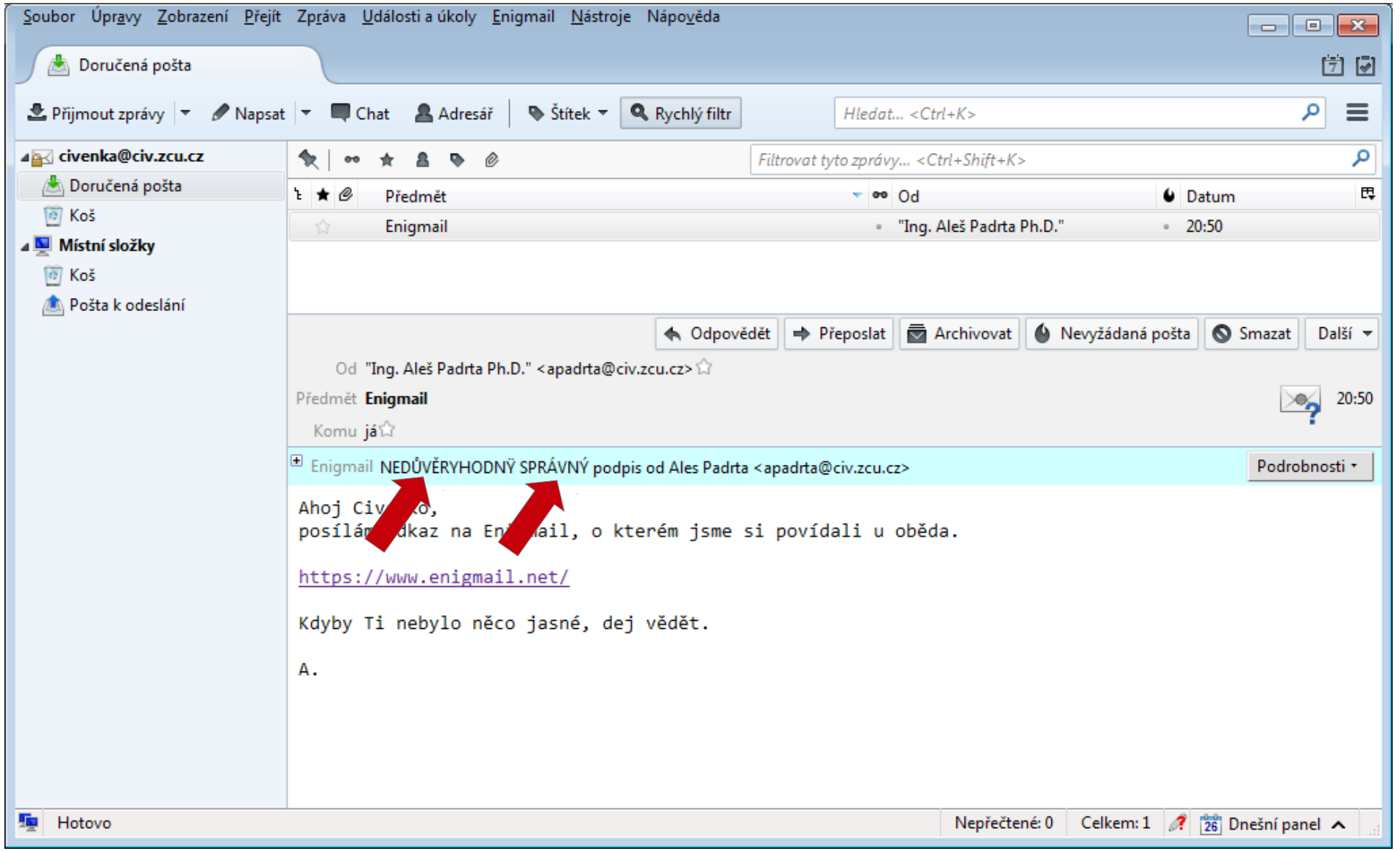
Import klíče pro doručený e-mail



Import klíče pro doručený e-mail

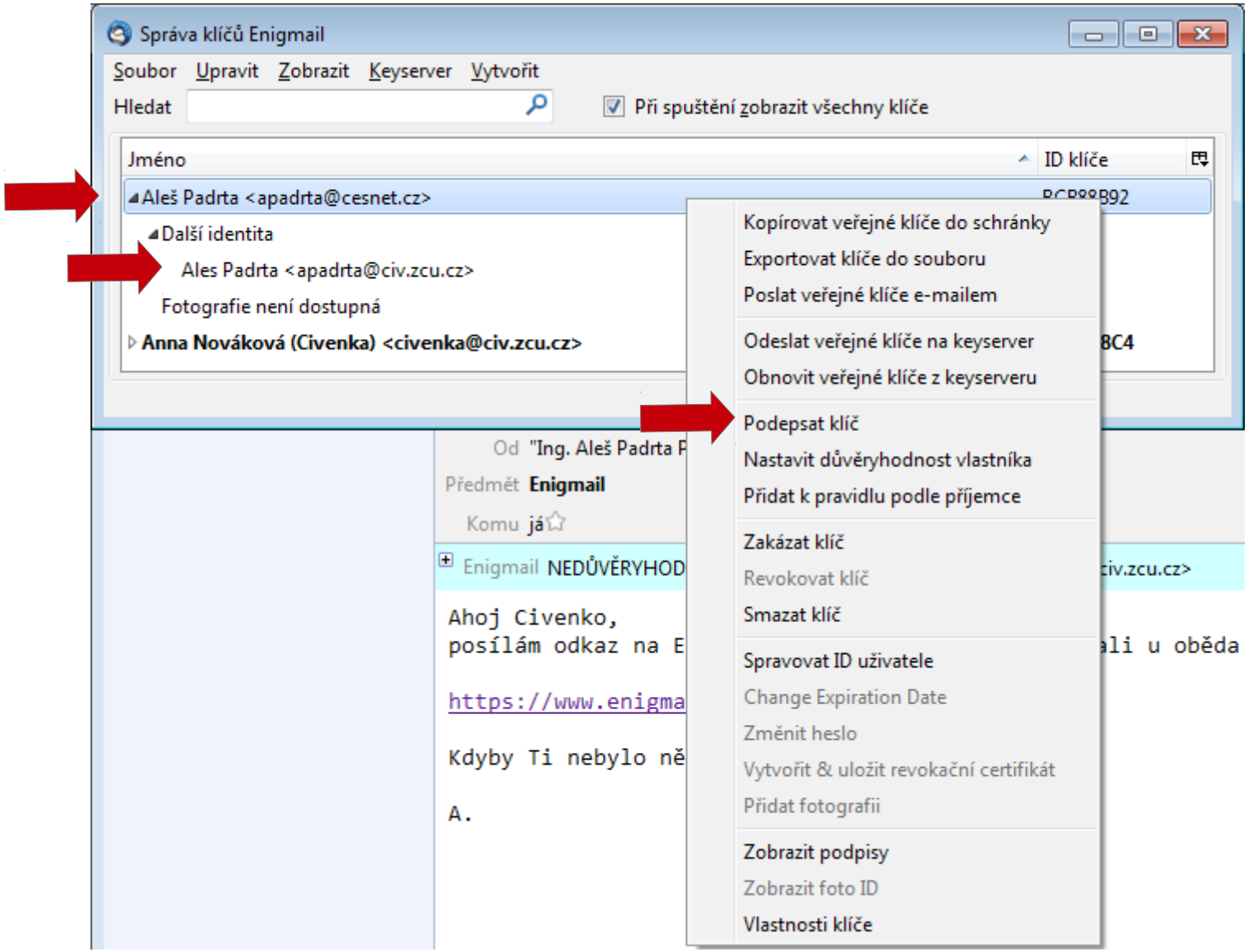


Neověřený importovaný klíč

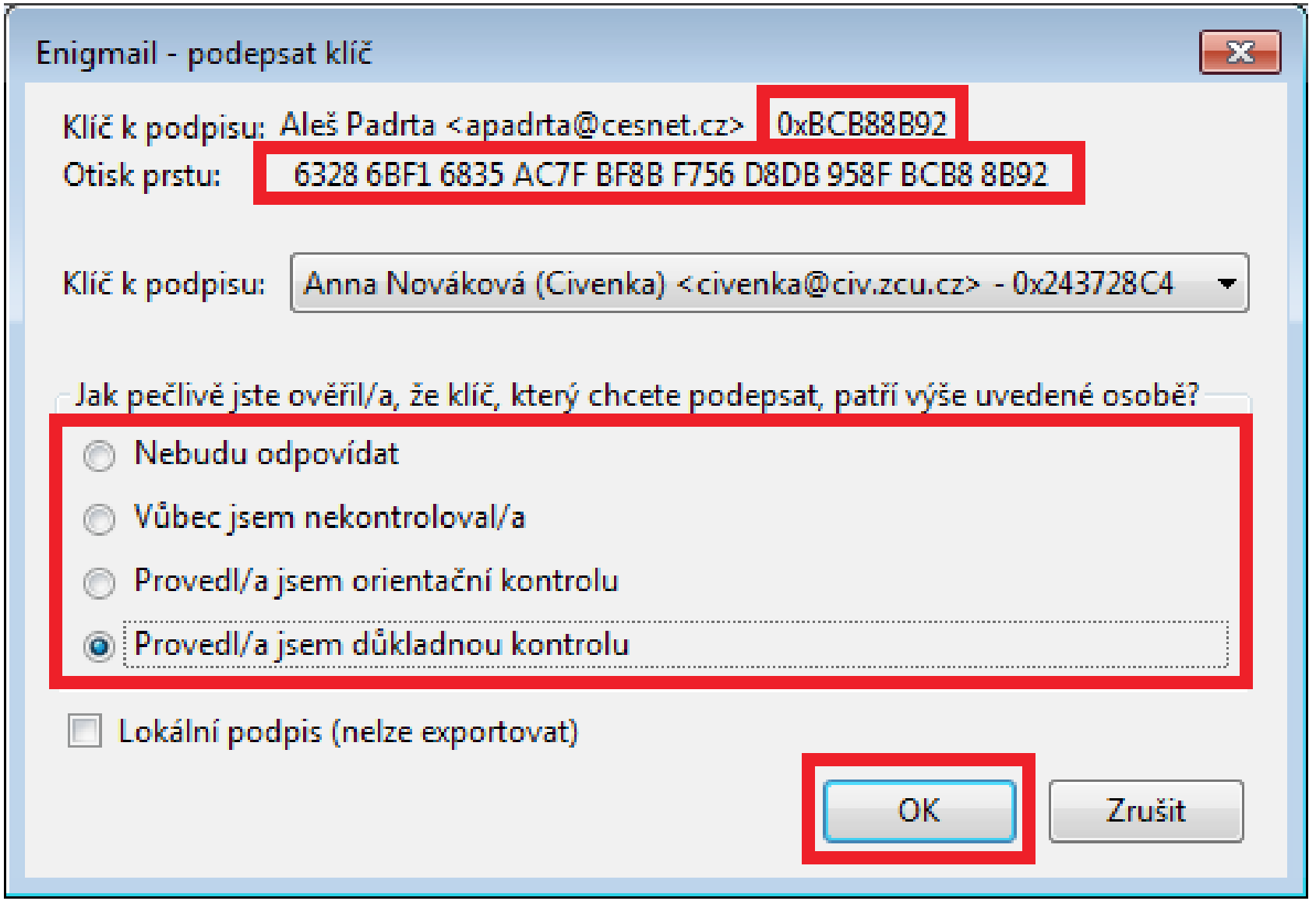


Kontrola otisku klíče

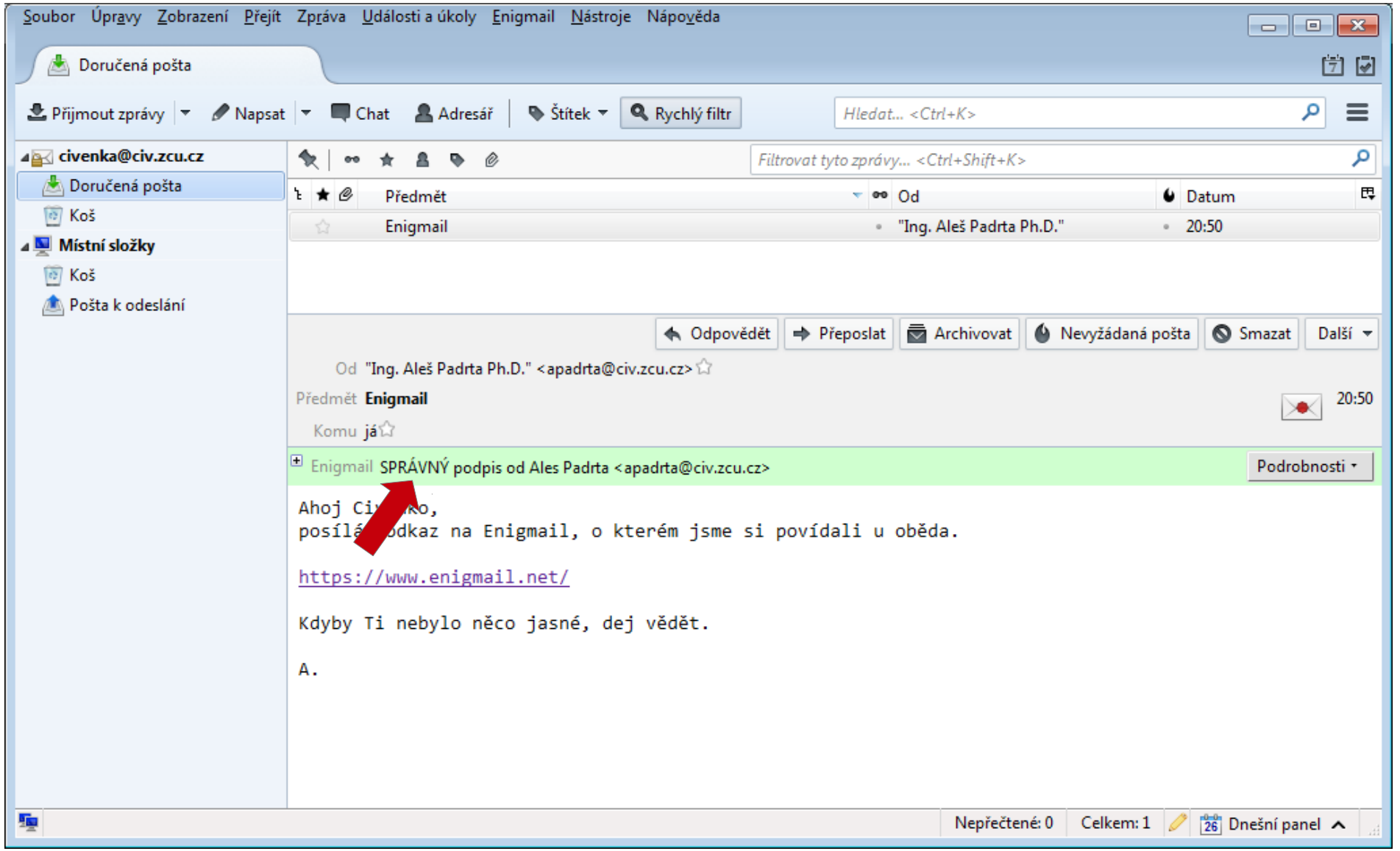
Ověření a podpis klíče



Ověření a podpis klíče

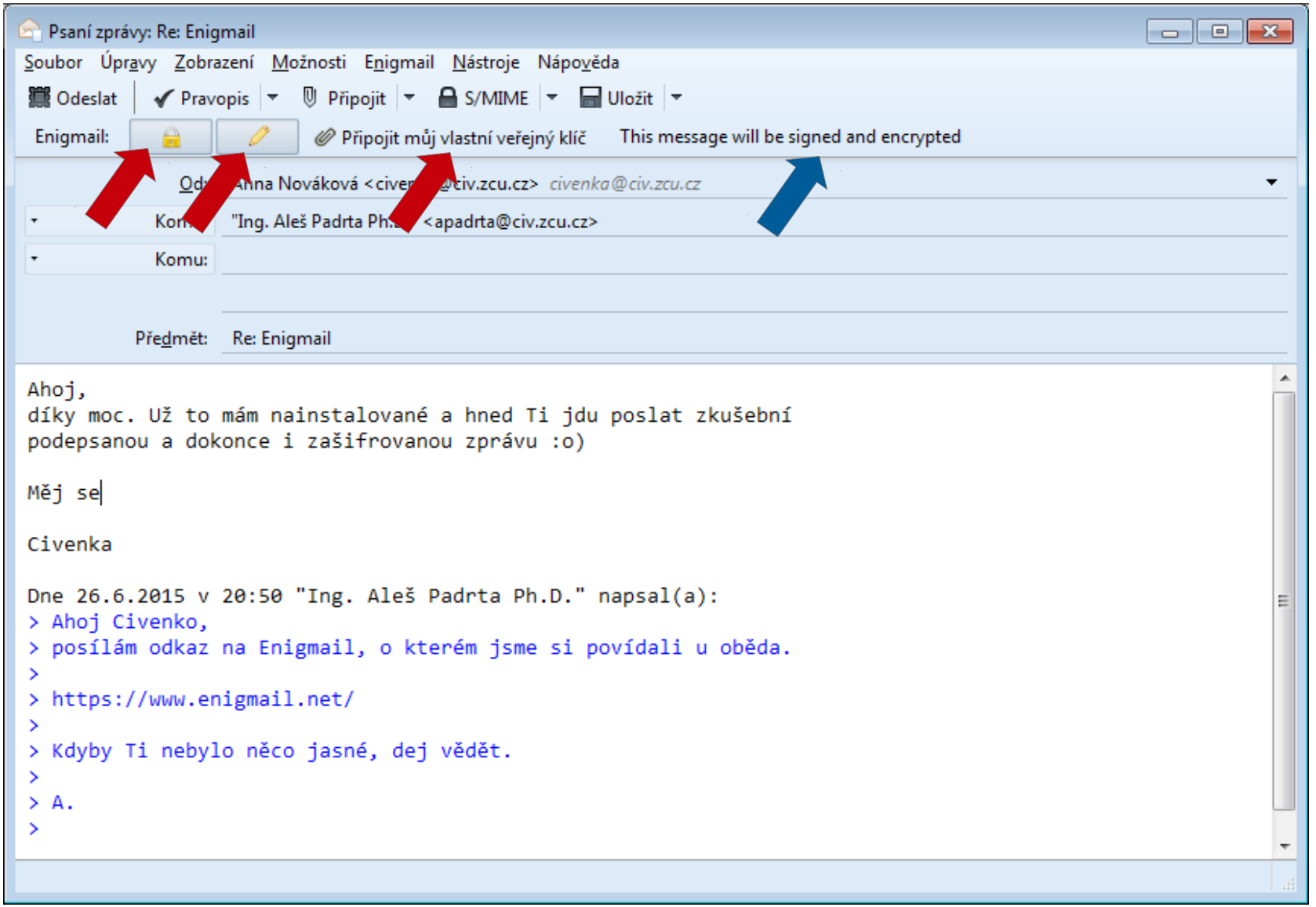


Odesílatel je ověřen

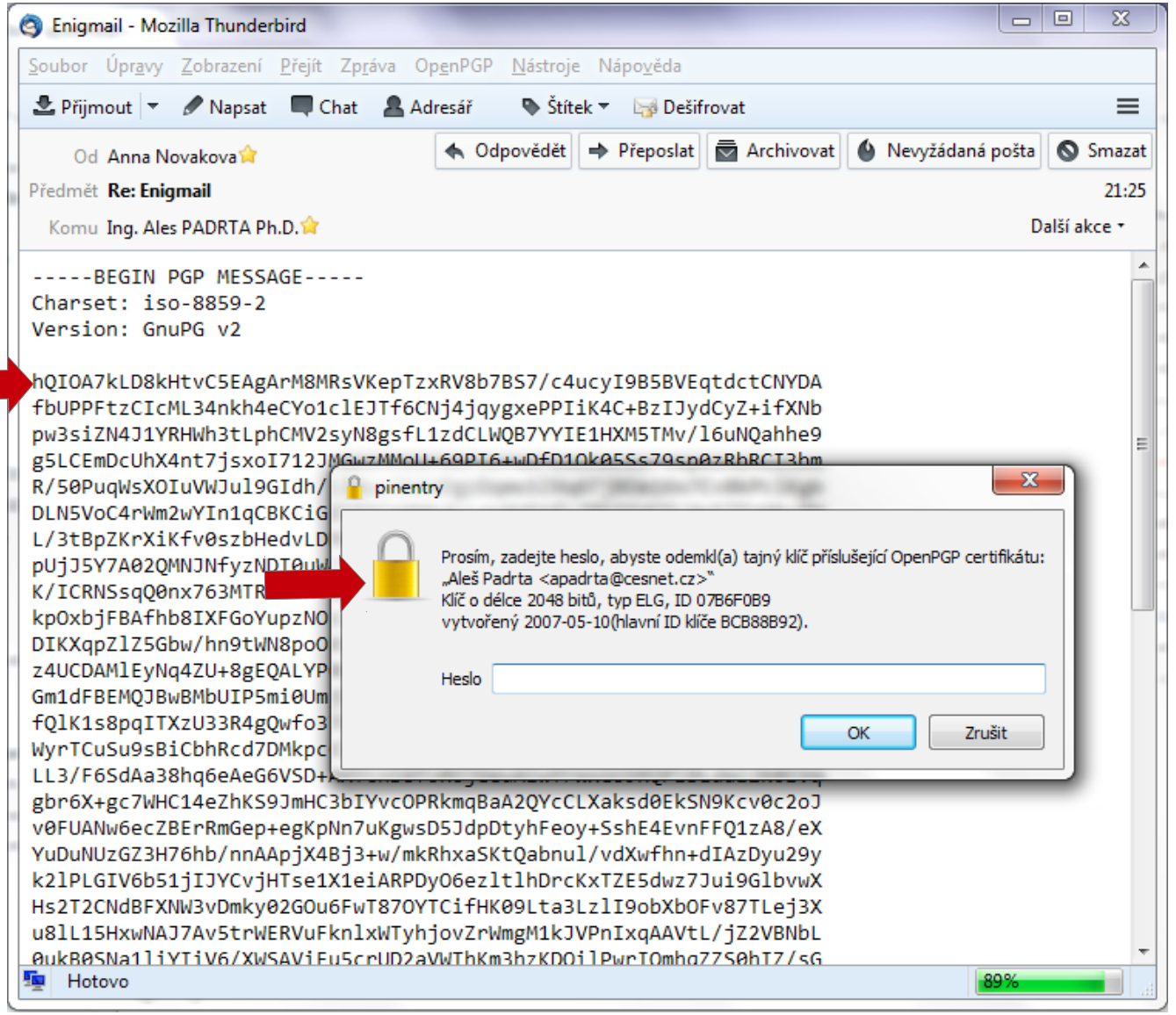


Civenka odesílá zprávu

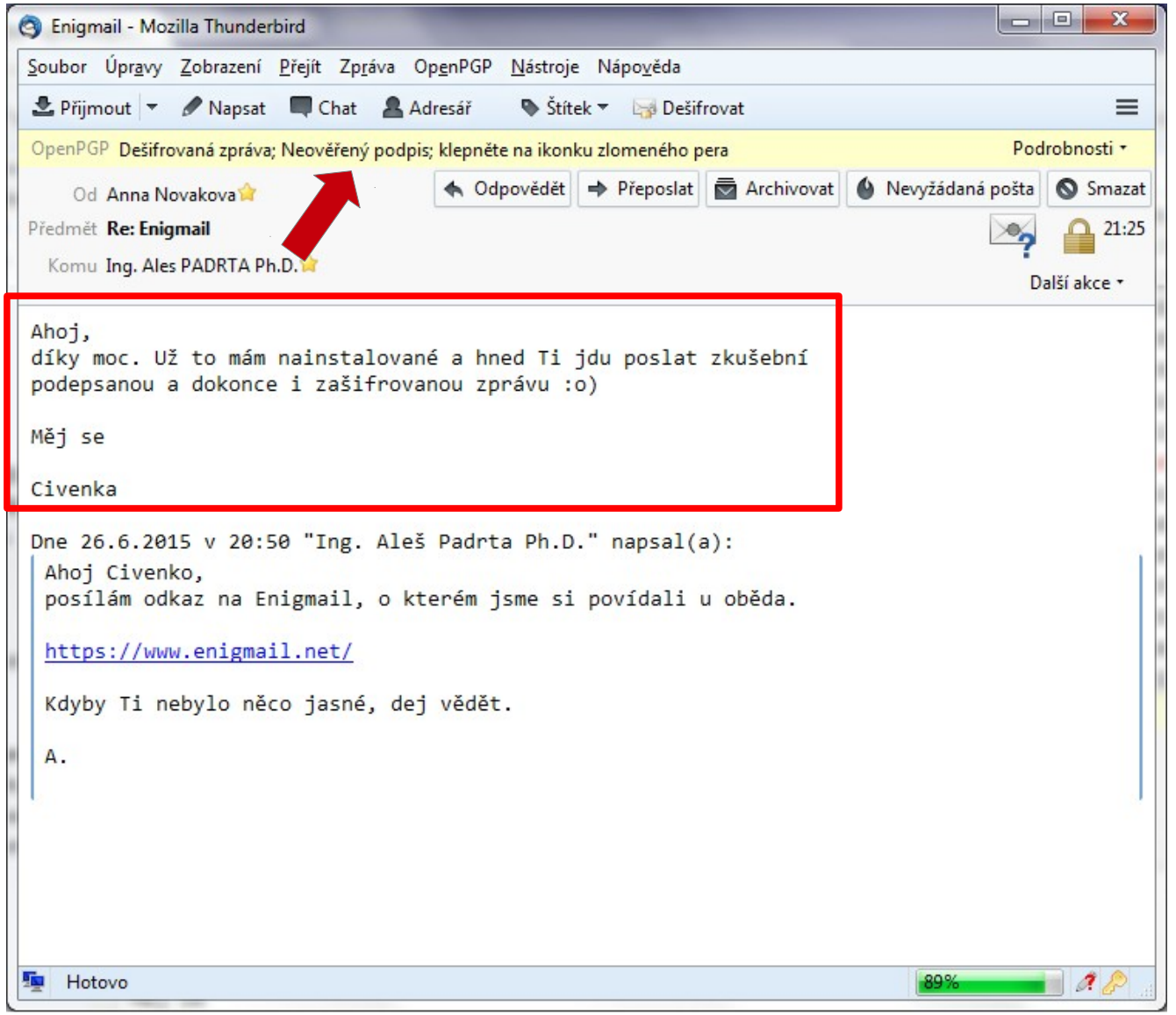
Civenka odesílá zprávu



Co je doručeno adresátovi?



Dešifrováno … a neověřeno



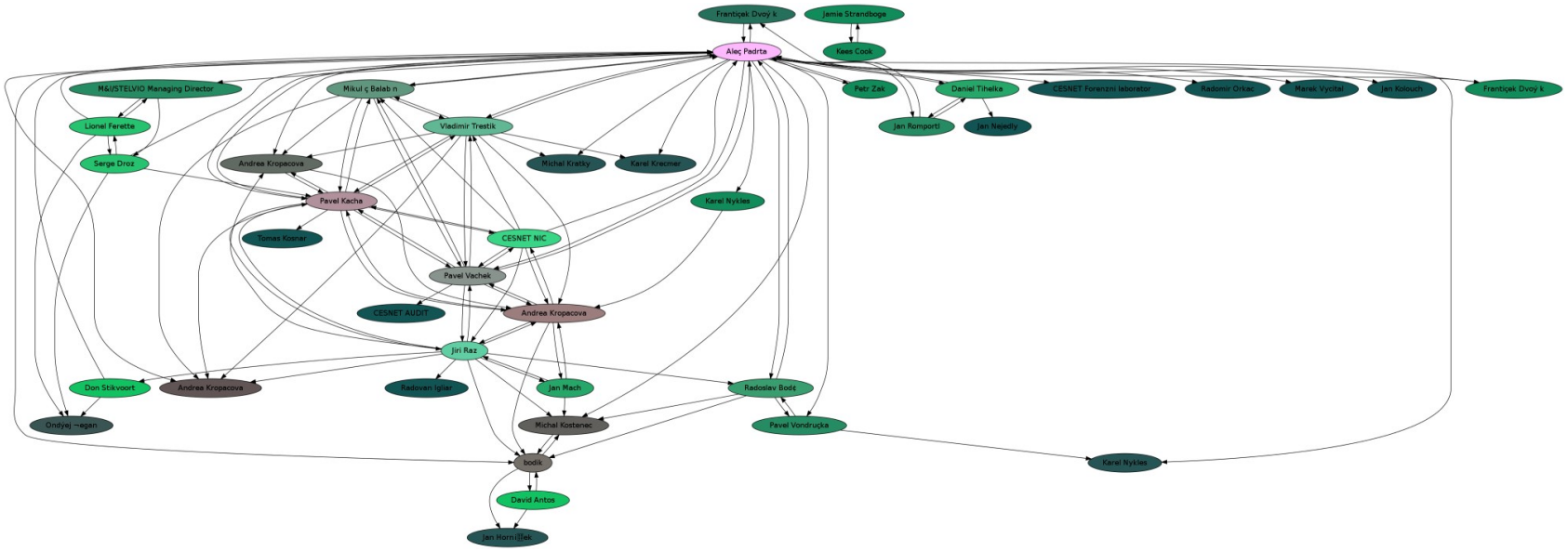
Další užitečné možnosti

- Jeden PGP klíče pro více e-mailových adres
- Export/Import veřejných/privátních klíčů
- Pravidla pro spárování klíčů a e-mailových adres
  - Implicitně = e-mailu uvedený u klíče
  - Při více identitách – občas potřeba ruční pravidlo
- Zobrazení informace o podpisech
  - Kdo všechno podepsal veřejný klíč
  - Verze 1.8.x – umí rovnou stáhnout informace o podpisech
  - Verze 1.9.x – info o podpisech je nutno stáhnout ručně

Vizualizace vazeb

- Sig2dot
  - http://www.chaosreigns.com/code/sig2dot/

```
# apt-get install graphviz
# apt-get install sig2dot
$ gpg --list-sigs | sig2dot > gpg.dot
$ dot -Tpng -Gcharset=latin1 gpg.dot > gpg.png
```



Shrnutí

- PGP
  - Pretty Good Privacy
  - Princip fungování
- GnuPG
  - Použití z příkazové řádky
- Enigmail
  - Rozšíření pro Mozillu Thunderbird
- Bezpečné komunikaci 3x hurá

Odkazy pro další studium

- https://www.gnupg.org/gph/en/manual.html
- http://www.spywarewarrior.com/uiuc/gpg/gpg-com-0.htm
- https://futureboy.us/pgp.html
- https://cs.wikipedia.org/wiki/Phil_Zimmermann
- http://www.root.cz/serialy/gnupg-komunikace-po-internetu-bezpecne/
- http://support.zcu.cz/index.php/PGP_-_Pretty_Good_Privacy
- http://support.zcu.cz/index.php/Enigmail

Diskuse, dotazy, ...