evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**

# Praktické šifrování dat pomocí programu PGP

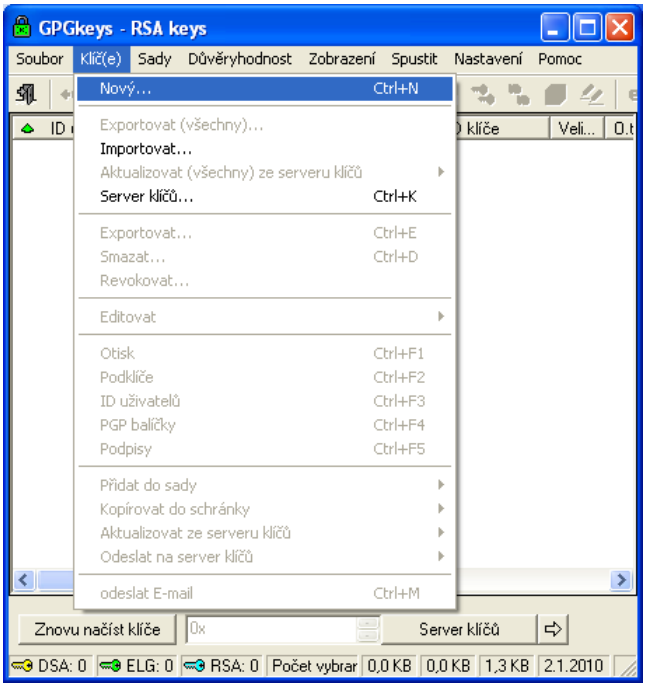
## Instalace prostředí

Jako první je nutné stáhnout program GPG a extrahovat jeho obsah do vybraného adresáře. Program získáme např. na adrese http://www.gnupg.org/ .

Ve druhé fázi je nutné stáhnout a nainstalovat grafickou nástavbu GPGshell. K tomu můžeme využít např. stránku autora http://www.jumaros.de . Důležité je,aby instalace proběhla do stejného adresáře, ve kterém je instalován program PGP. Dále je si nutné ověřit zpětnou kompatibilitu obou prostředí ( pokud použijeme starší verzi programu PGP, nemusí s ním být PGPshell kompatibilní). Tyto údaje jsou uvedeny na stránkách autora programu. Důležitým údajem je, že celá grafická nástavba obsahuje české rozhraní.

## Vytvoření klíčů

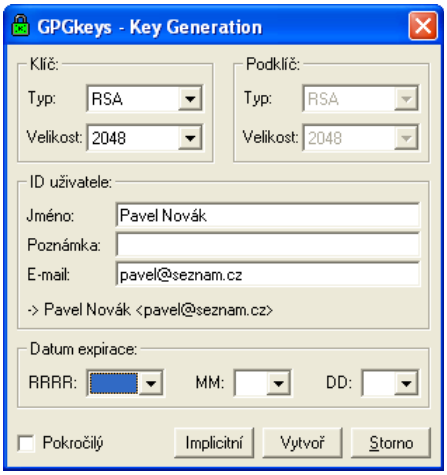
Spustíme program GPGkeys  Klíč(e)  Nový



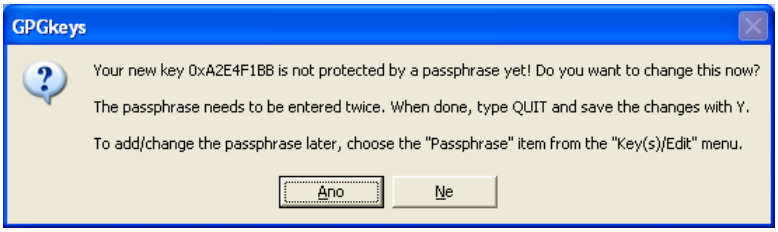
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**

Nyní se otevře nabídka, pomocí které budeme moci vytvořit elektronický klíč.



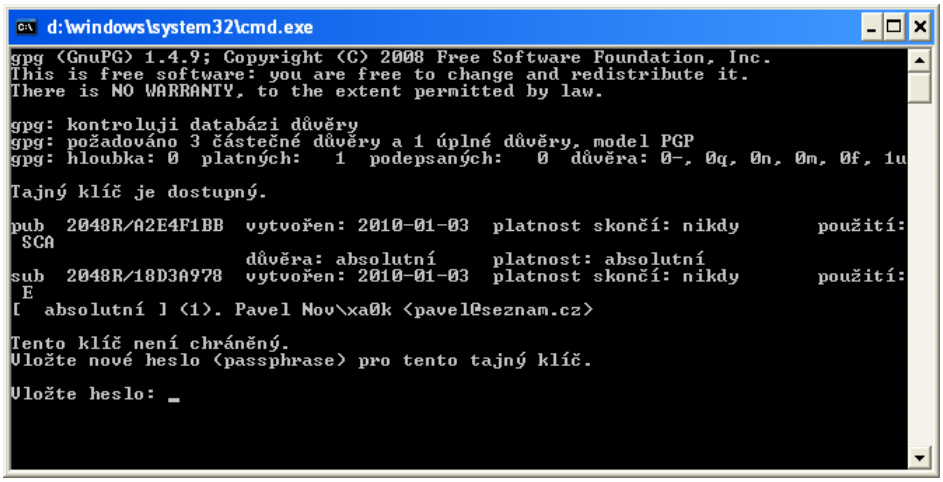

Zde je nejdůležitější vyplnit identifikační údaje uživatele, případně datum expirace (ukončení platnosti) elektronického klíče. Potvrdíme klávesou **Vytvoř.**



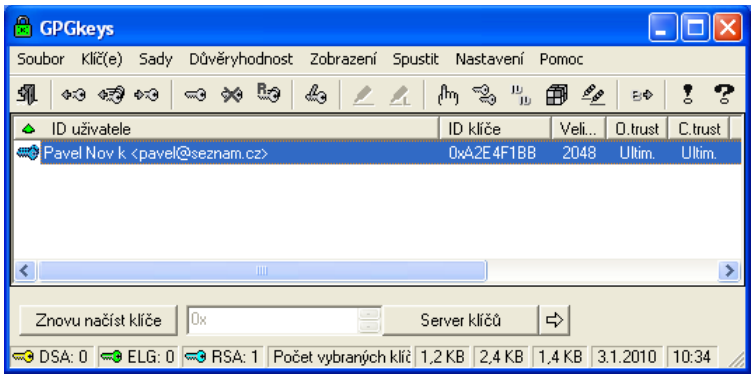

Následující okno potvrdíme tlačítkem **ANO** – vytvoříme si tak heslo, pomocí kterého bude chráněn elektronický podpis a šifrovány data.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




Po opakovaném zadání hesla zavřeme aktuální okno příkazového řádku.



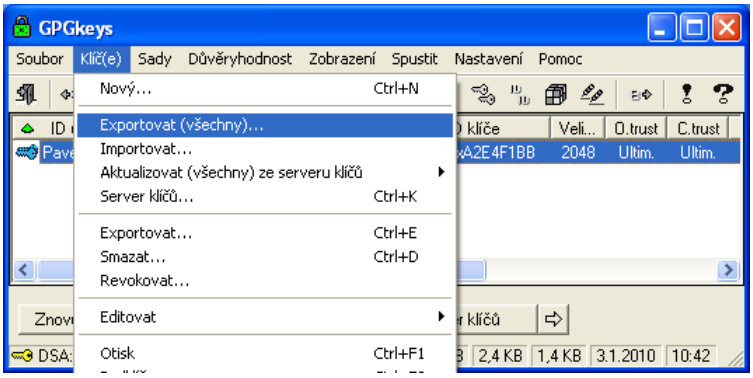

Klíče jsou vytvořené.

**Export veřejného a soukromého klíče**

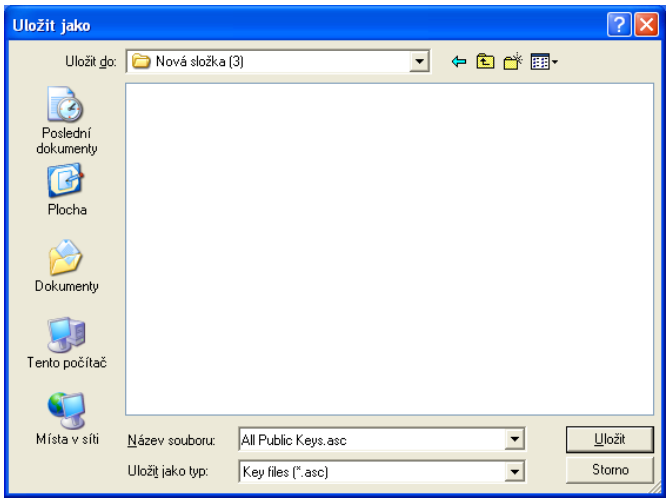
Důležité upozornění – veřejný klíč lze kdekoliv veřejně vystavit, slouží pouze k zašifrování dat. Soukromý klíč musí být uložen na bezpečném místě. Pokud je vystaven krátkodobě, měl by mít nastaven datum expirace. Při případném odhalení soukromého klíče musí být vygenerovány nové páry klíčů. Starý klíč by měl být revokován.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




V prvním kroku označíme klíč, který chceme generovat a nastavíme Klíč(e)  Exportovat(všechny).

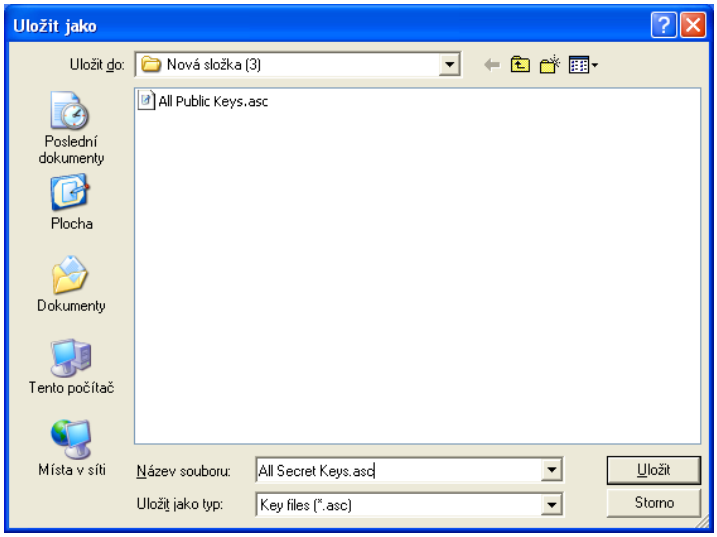



Jako první ukládáme veřejný (Public) klíč.


Nabídka vytvoření tajného (secret) klíče. Zvolíme **ANO**.

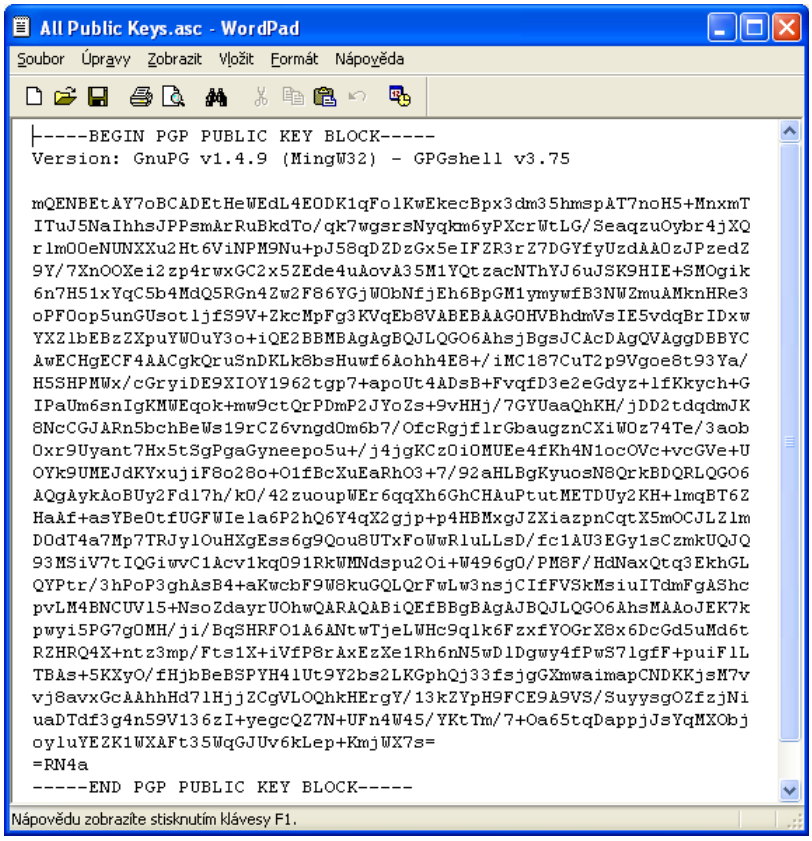
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




Secret (tajný) klíč uložíme na bezpečné místo na disku. Nyní máme vygenerovaný veřejný i soukromý klíč, které tvoří tzv. klíčový pár.

Příklad výpisu veřejného klíče:




## Import cizího veřejného klíče

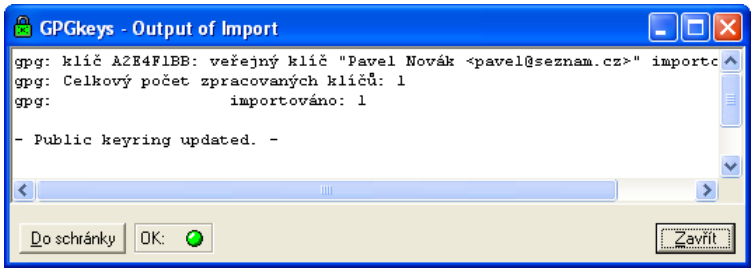
Používá se tehdy, chceme-li někomu zašifrovat zprávu tak, aby byla dešifrována pouze určenou osobou, která má příslušný soukromý klíč.

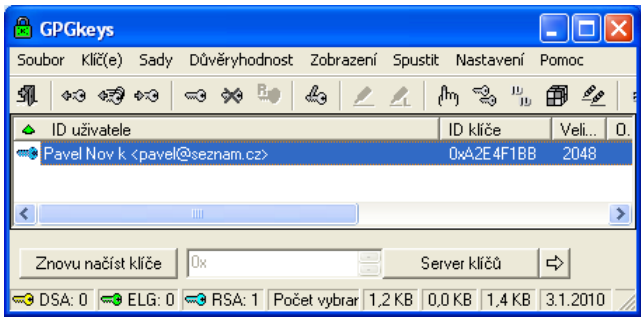
V první fázi musíme příslušný veřejný klíč získat – prostřednictvím internetu, CD, serveru klíčů apod.

Dále jej importujeme podle následujících kroků.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**

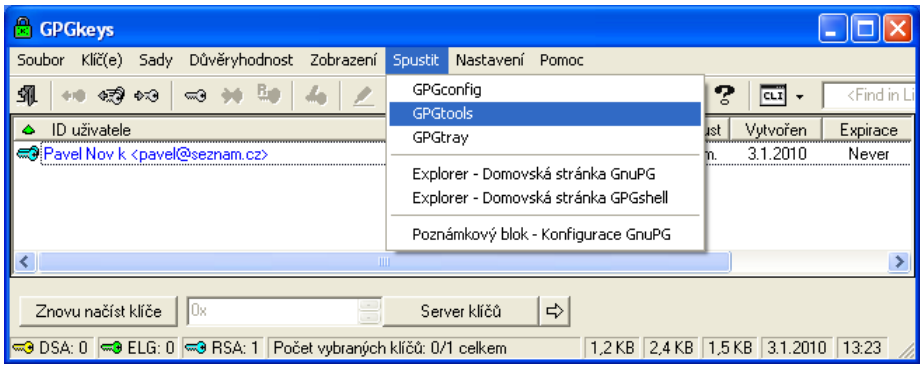



Import klíče je hotový.

## Šifrování dat

Prvním předpokladem je importovaný veřejný klíč osoby, které budeme šifrovat data. Pak již provádíme samotné šifrování.

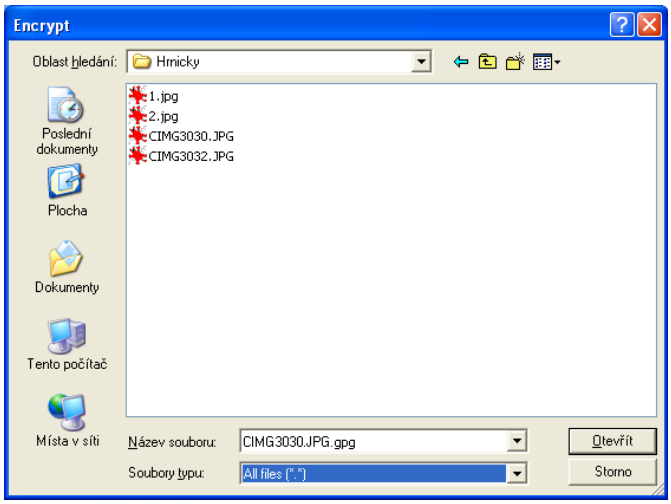



Spustíme si okno panelu nástrojů, které nám umožní provést proces šifrování dat.

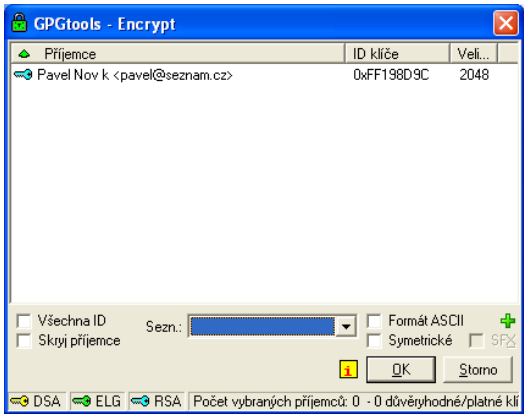
evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**

Šifrování dat



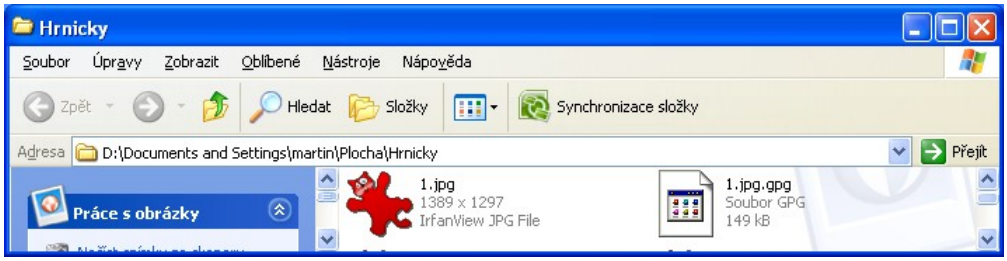

Následně vybereme soubor, který chceme zašifrovat.




Pak vybereme příjemce, kterému budeme soubor šifrovat a potvrdíme. Soubor je zašifrován.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

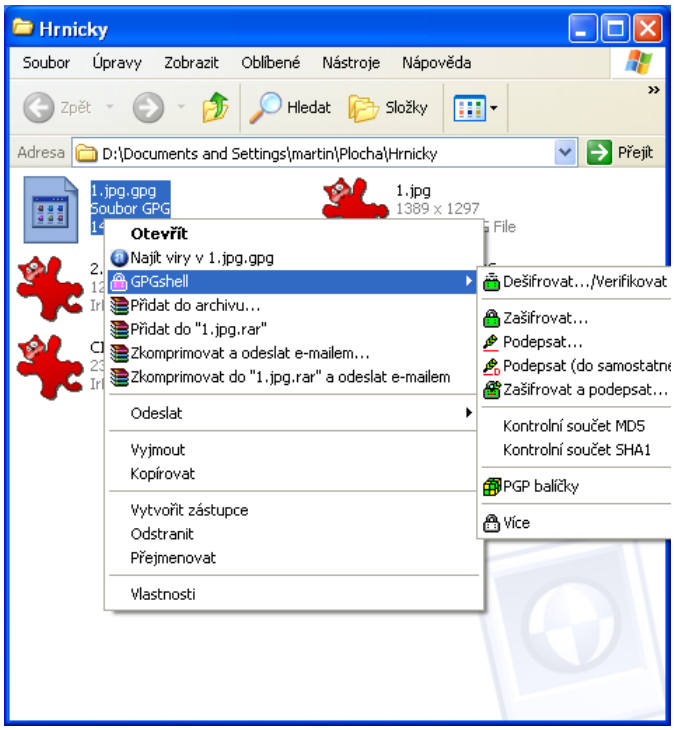
**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




původní soubor zašifrovaný soubor

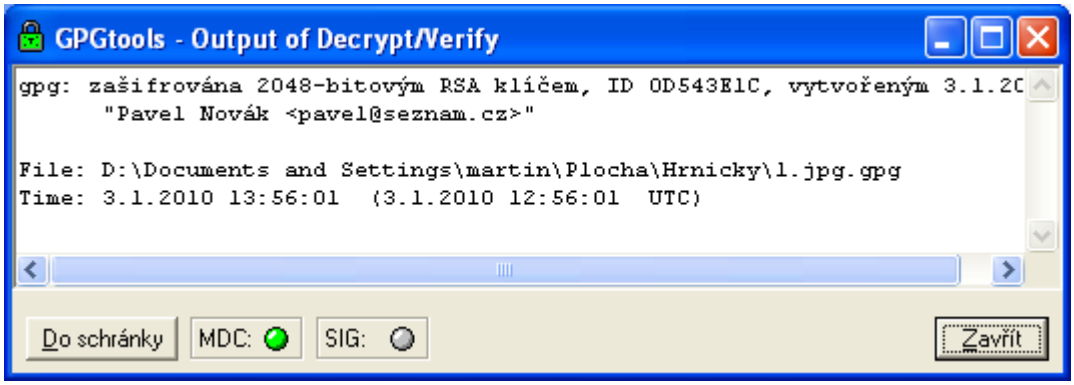
**Dešifrování souboru**

Můžeme provést prostřednictvím nabídky GPGtools nebo pomocí volby pravého tlačítka myši – GPGshell  Dešifrovat



evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




Tabulka, podívající stručné informace o procesu šifrování. Soubor je dešifrován.

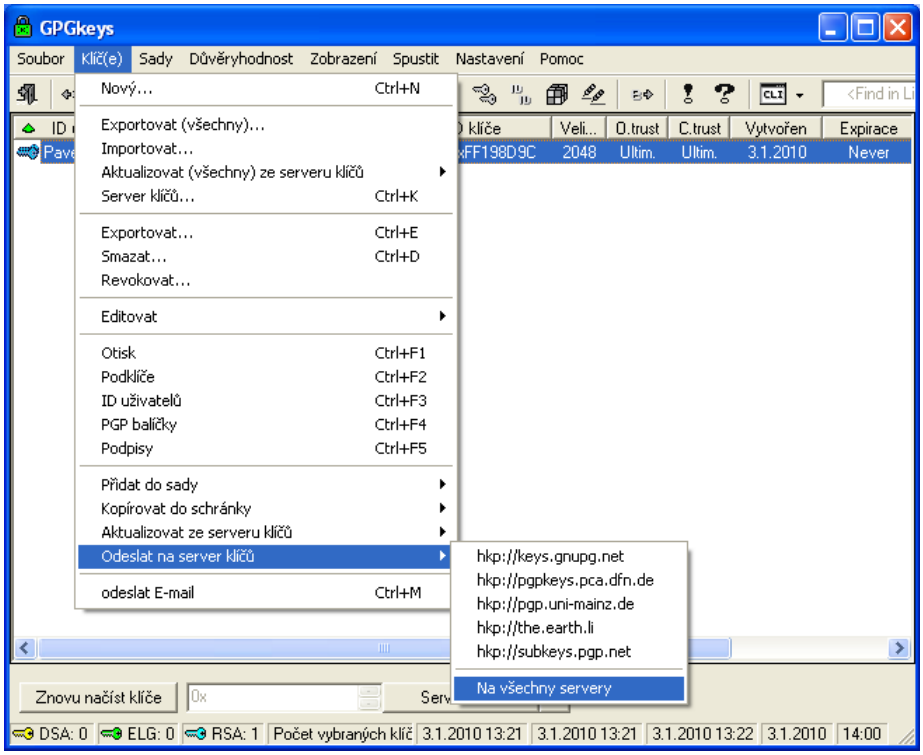
Podmínkou úspěšného dešifrování je existence soukromého klíče.

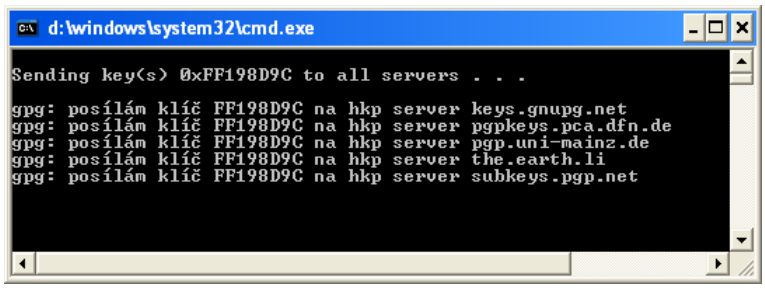
**Práce se serverem klíčů**

Pokud chceme veřejně zpřístupnit náš veřejný klíč, není jednodušší možnost, než ho zveřejnit na server klíčů.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**

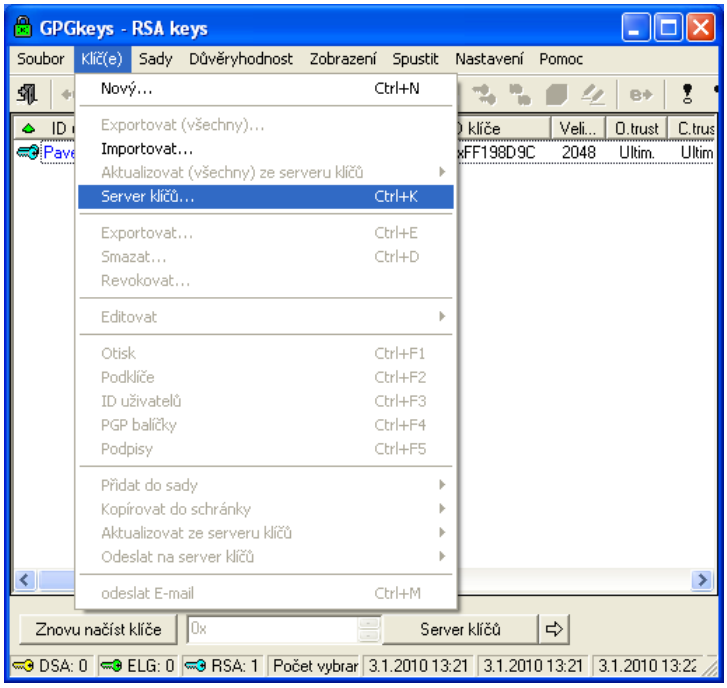


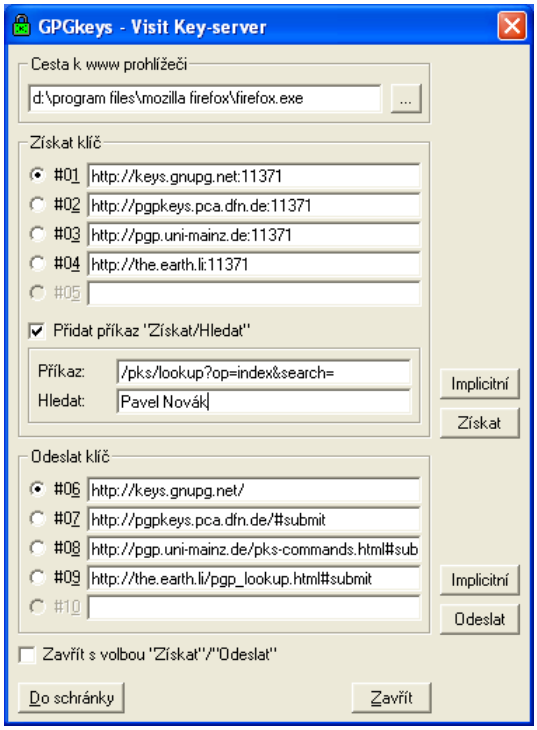




Následně jsou klíče zaslány na všechny příslušné servery. Pokud chceme najít příslušný veřejný klíč a stáhnout si ho pro šifrování dat, je nutné znát název klíče. Celá akce se provádí prostřednictvím serveru klíčů.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**




Do pole **Hledat** napíšeme název klíče a stiskneme tlačítko **Získat**.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**Projekt: 1.5, Registrační číslo: CZ.1.07/1.5.00/34.0304**


Nyní máme vypsané všechny klíče, které jsou na serverech k dispozici. Prostřednictvím hypertextového odkazu si je můžeme uložit a jejich prostřednictvím šifrovat daným osobám data.

**Použitá literatura:**

DOLEŽAL, Martin. *Šifrování dat a elektronický podpis* [online]. [cit. 2013-02-03]. Dostupné z: http://coptel.coptkm.cz/index.php?action=2&doc=1532&docGroup=209&cmd=0&instance=1

*Using the GNU Privacy Guard* [online]. 2012. vyd. [cit. 2013-02-03]. Dostupné z: http://www.gnupg.org/documentation/manuals/gnupg/