



PERSI EMPLOYER TRANSMITTAL PROCEDURE

Each of the PERSI Employers not using PETRA are required to transmit (Upload) their monthly statements via Email using PGP encryption. The following is a step-by-step procedure of how the process will work and what will be required of the respective Employers to upload their export files to PERSI.

History

When PERSI installed HREdge in 2001 we began to require employers to encrypt transmittal files using PGP encryption. At the time PGP version 6.5.1 was open source and free. This version contained a command line processor so encryption/decryption tasks could be automated. Soon there after PGP Corporation was formed, and took over the maintenance of the PGP software. Although you can still get a free version of the PGP software the original functionality of the program was split up with some features becoming separate for fee services. Given this situation, PERSI has explored the use of alternative PGP software, and is recommending converting to Gpg4win. Based on our own testing, current functionality is preserved along with support for newer operating systems (Vista, Windows 7.0/8.0). The recommended version has a command line interface (although the scripting syntax is different). Although the name of the software starts with GPG, the product still uses PGP encryption.

OVERVIEW: A WORD ABOUT PGP

PGP[®] (or Pretty Good Privacy[®]) is a powerful cryptographic scheme that enables people to securely exchange messages, and to secure files, disk volumes, and network connections with both [privacy](#)* and *strong authentication*.

PGP is the world's *de facto* standard for email encryption and authentication, with over 6 million users.

***Privacy means that only the intended recipient of a message can read it. By providing the ability to encrypt messages, PGP provides protection against anyone eavesdropping on the network. Even if the information is intercepted, it is completely unreadable to the snooper. Authentication identifies the origin of the information, certainty that it is authentic, and that it has not been altered. Authentication also provides an extremely valuable tool in network security: verification of the identity of an individual. In addition to secure messaging, PGP also provides secure data storage, enabling you to encrypt files stored on your computer.**

Installation instructions

Screenshots may differ from this document depending on your operating system.

1. Download software from web site. <http://www.gpg4win.org/download.html>
(current version as of 12/06/2012 was 2.1.0)
2. Close all other applications. Make sure that no other programs are running on your computer.
3. Double-click on the file you have downloaded and follow the instructions on the screen.

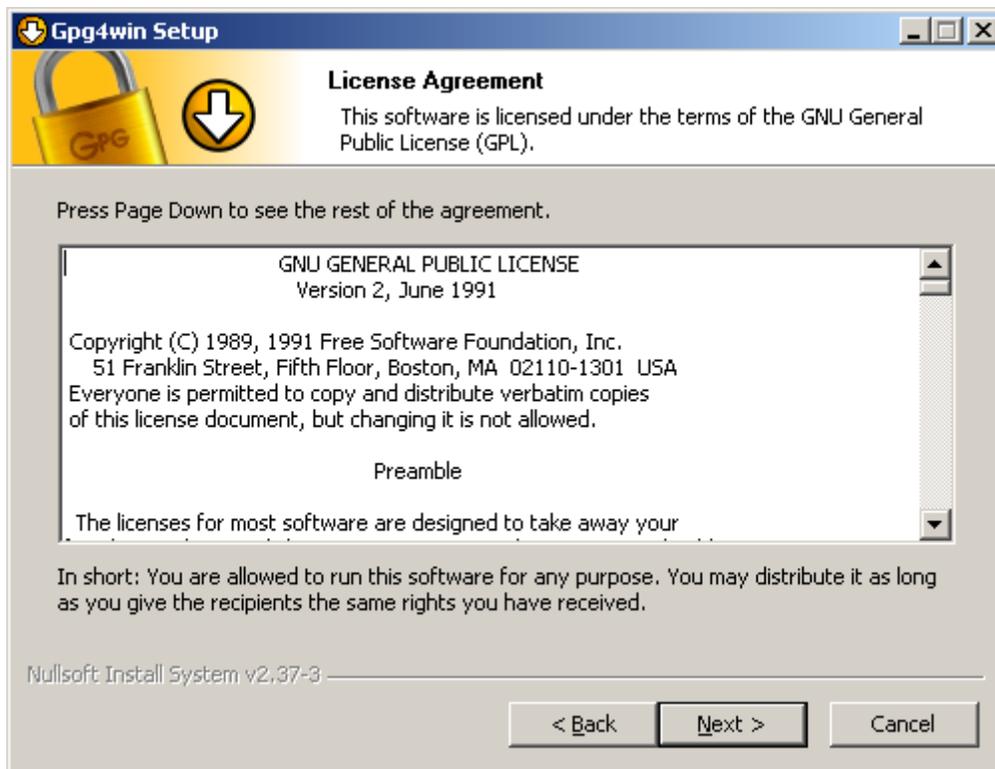


B. Select the install language and Click 'OK'.



A. Click Next.

4. Accept the license.



A. Click Next.

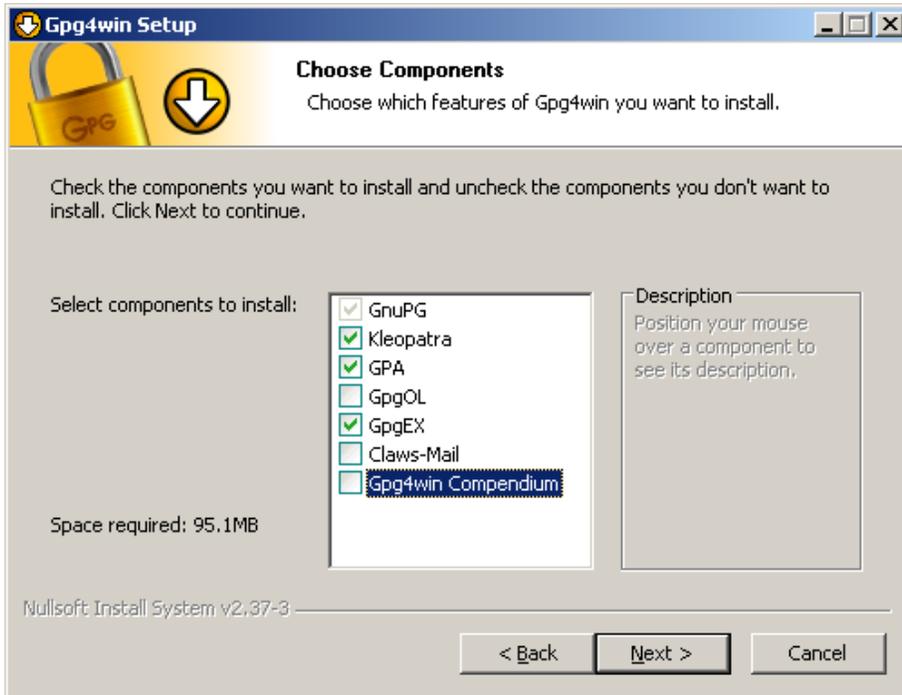
5. Choose the following software modules for installation.

GnuPG

Kleopatra (replacement for PGPTools)

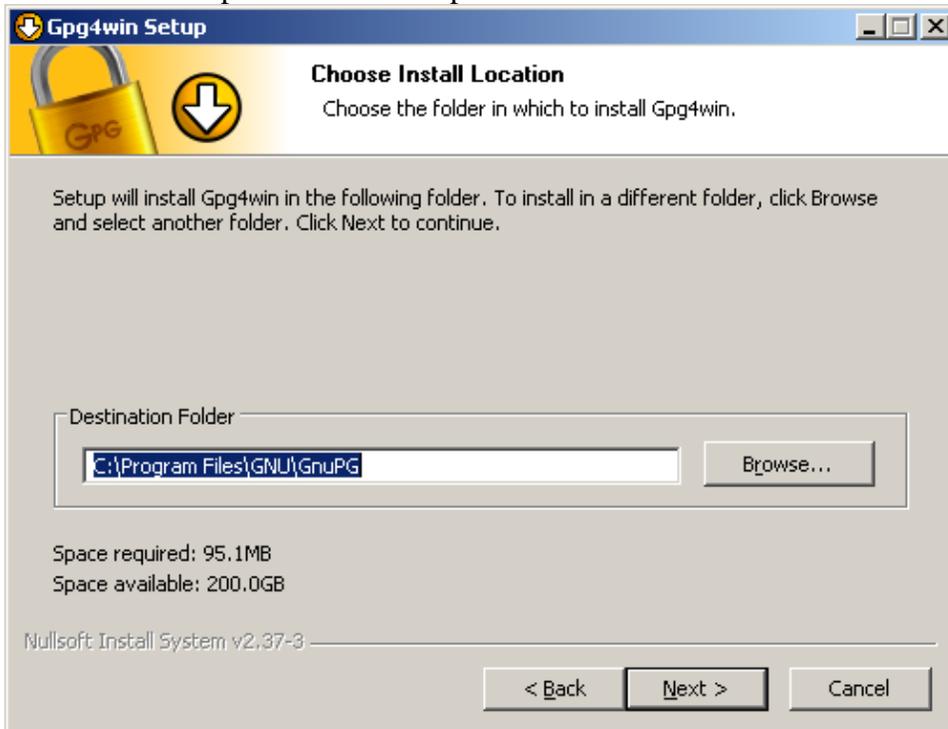
GPA (key manager)

GpgEx



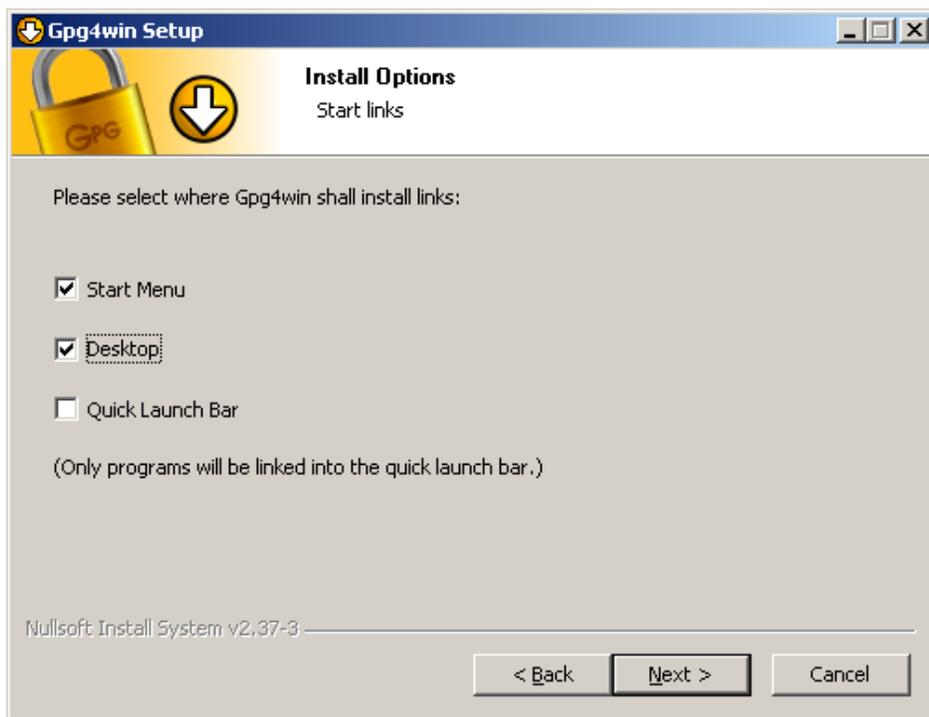
A. Click Next.

6. Enter or accept the installation path.



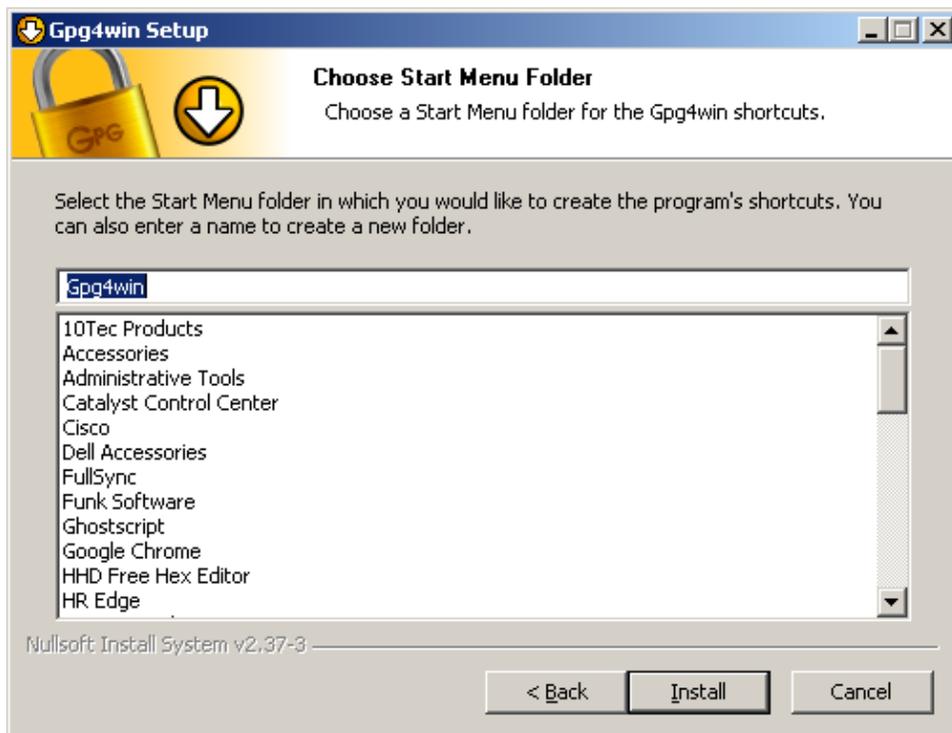
A. Click Next.

7. Choose the installation options.



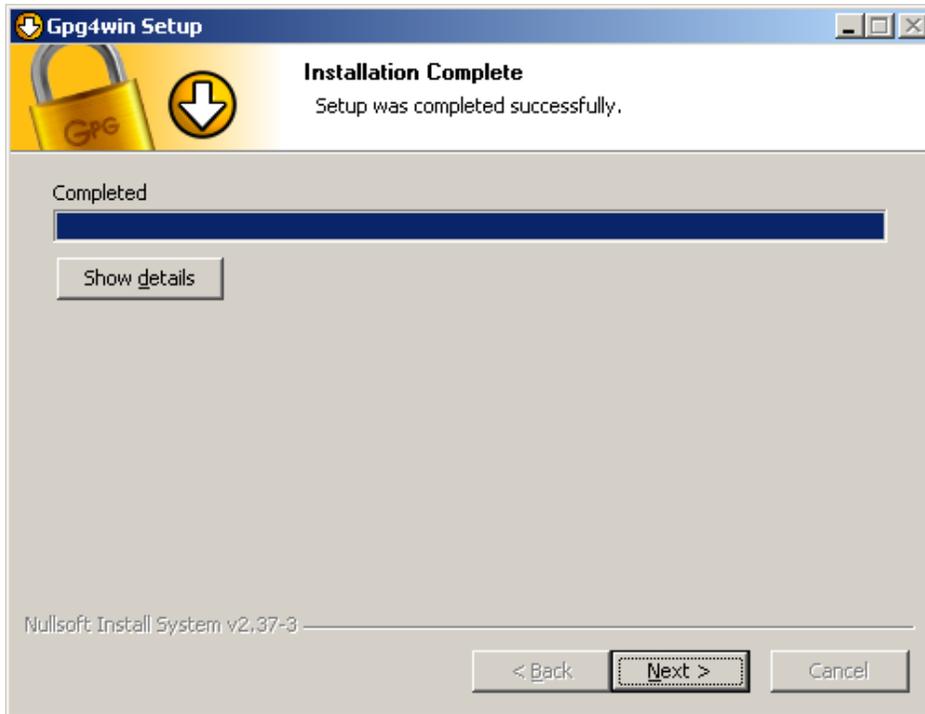
A. Click Next.

8. Choose an installation folder.



A. Click 'Install'. The software will be installed.

B. Click on OK if any warnings are issued.



C. Click on the 'Next' button.



D. Click the 'Root certificate defined or skip configuration' check box and then click the 'Next' button.

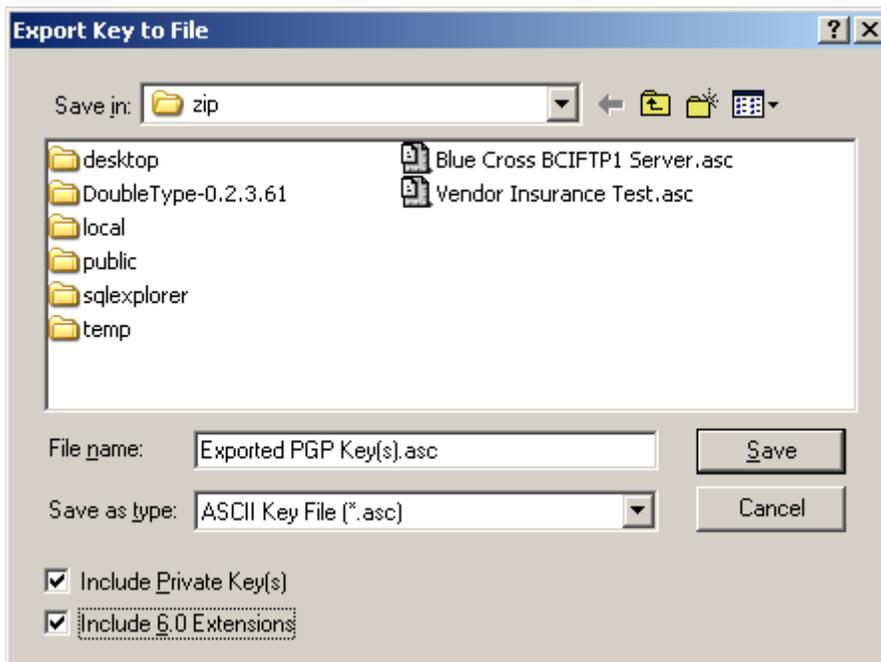
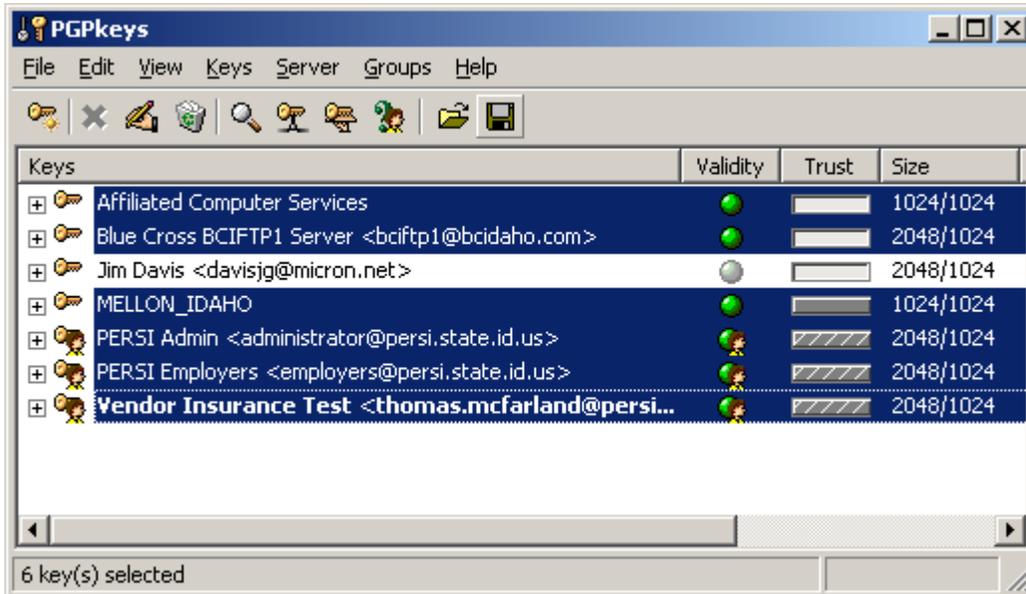
9. You may need to reboot your system depending on what is currently running while the installation takes place.



A. Click Finish. Then reboot, to complete the installation and update your system's path.

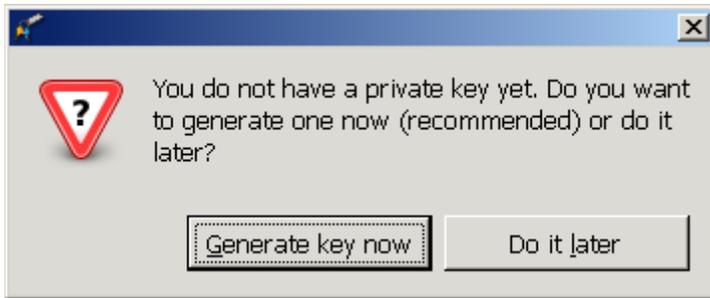
If you are converting from PGP to gpg4win continue. Otherwise, skip to step 12.

10. Export keys from PGP.
 - A. Start up the PGPKkeys application
 - B. Highlight the keys you would like to export.
 - C. Click the export icon.



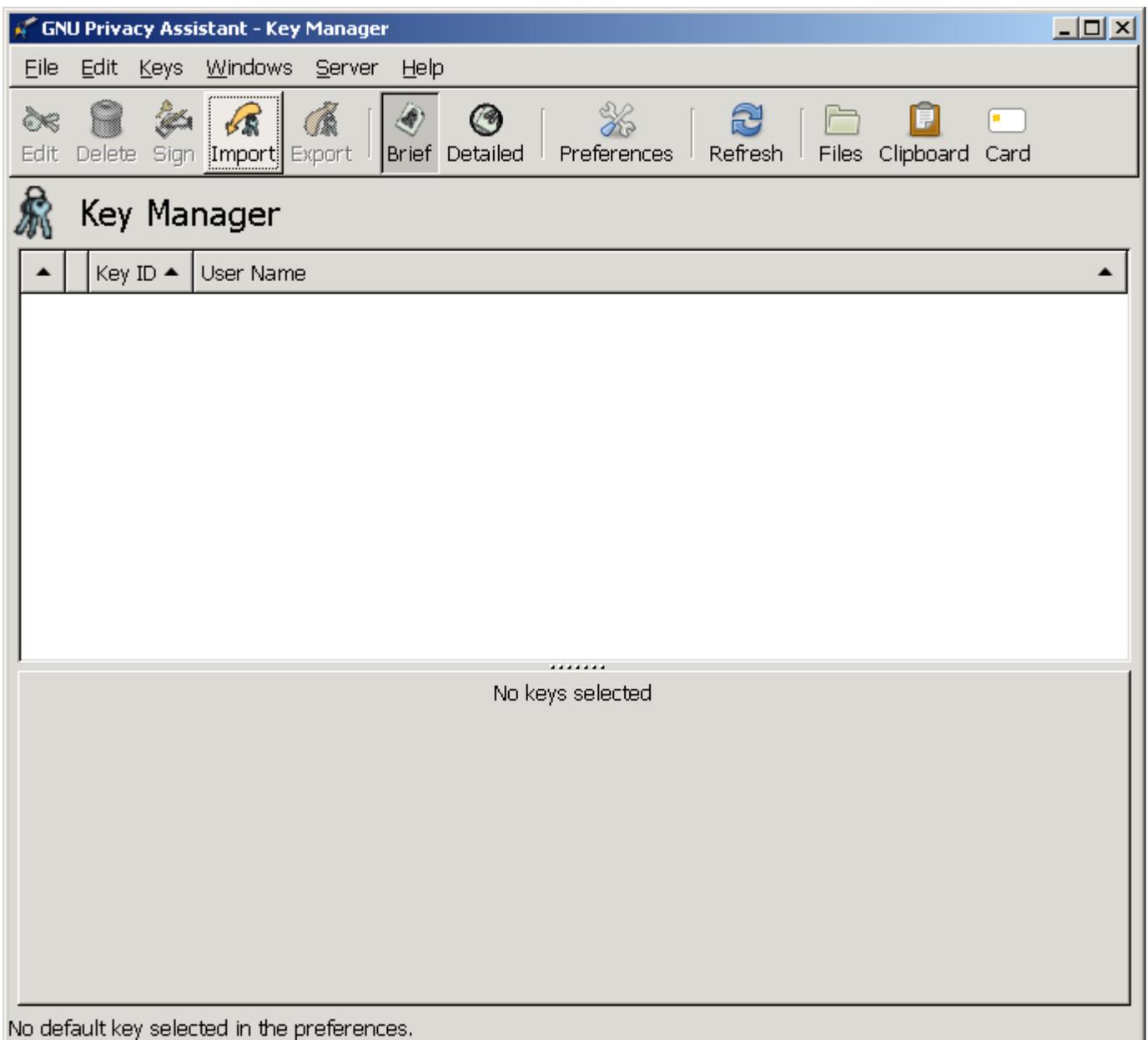
- D. Enter the File name.
- E. Check the include Private Key(s), and include 6.0 extensions check boxes.
- F. Click the Save button.

11. Import the keys into gpg4win.
Start the GPA application.

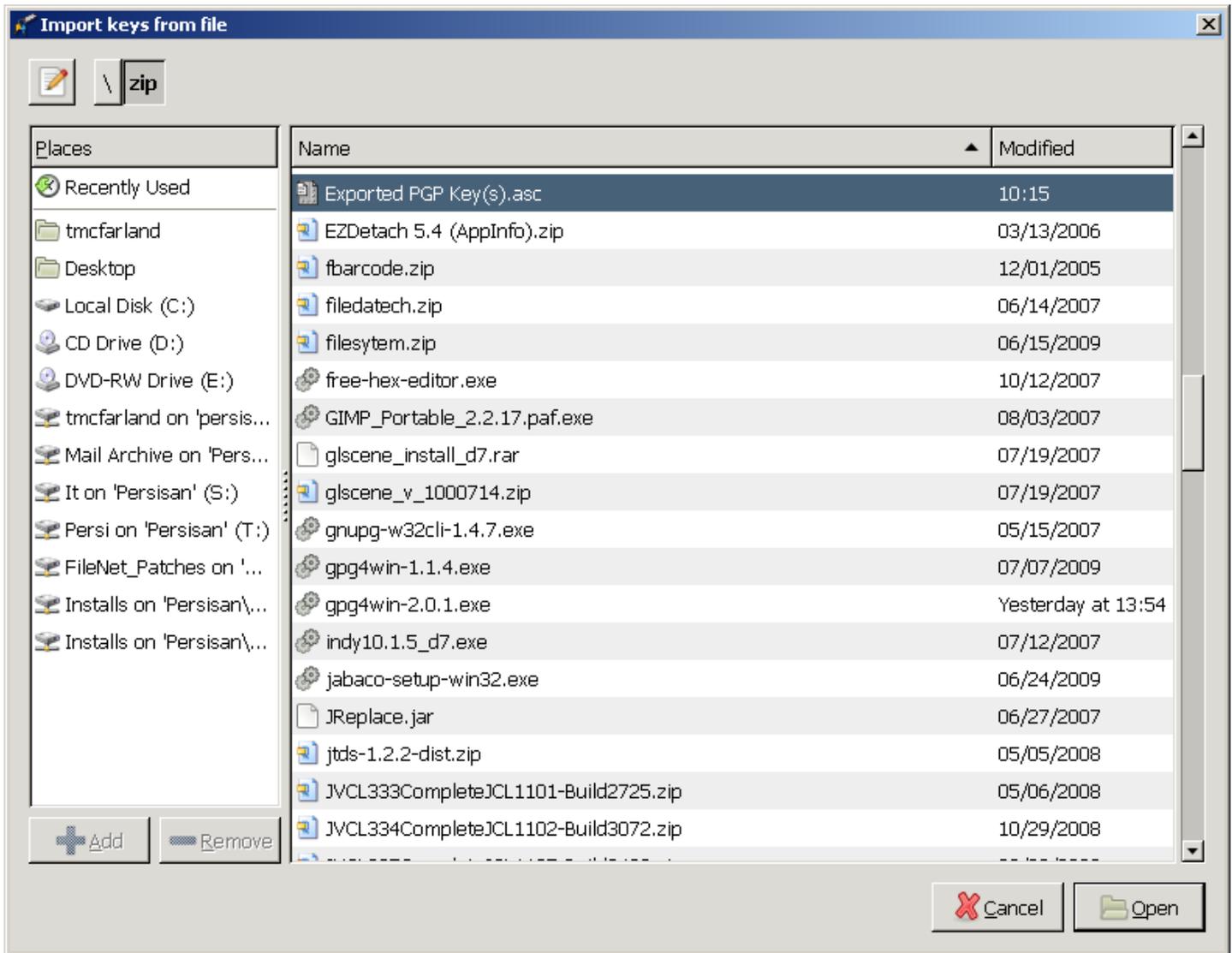


A. Click the “Do it Later” button.

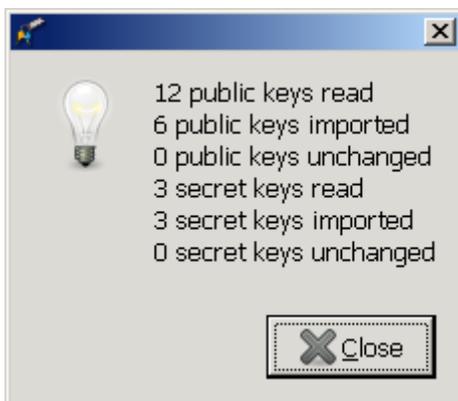
The GPA application will be displayed.



B. Click the import button in the tool bar.



C. Navigate to your exported pgp key file.
Highlight it, then click the Open button.



The keys will be imported.

GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card

Key Manager

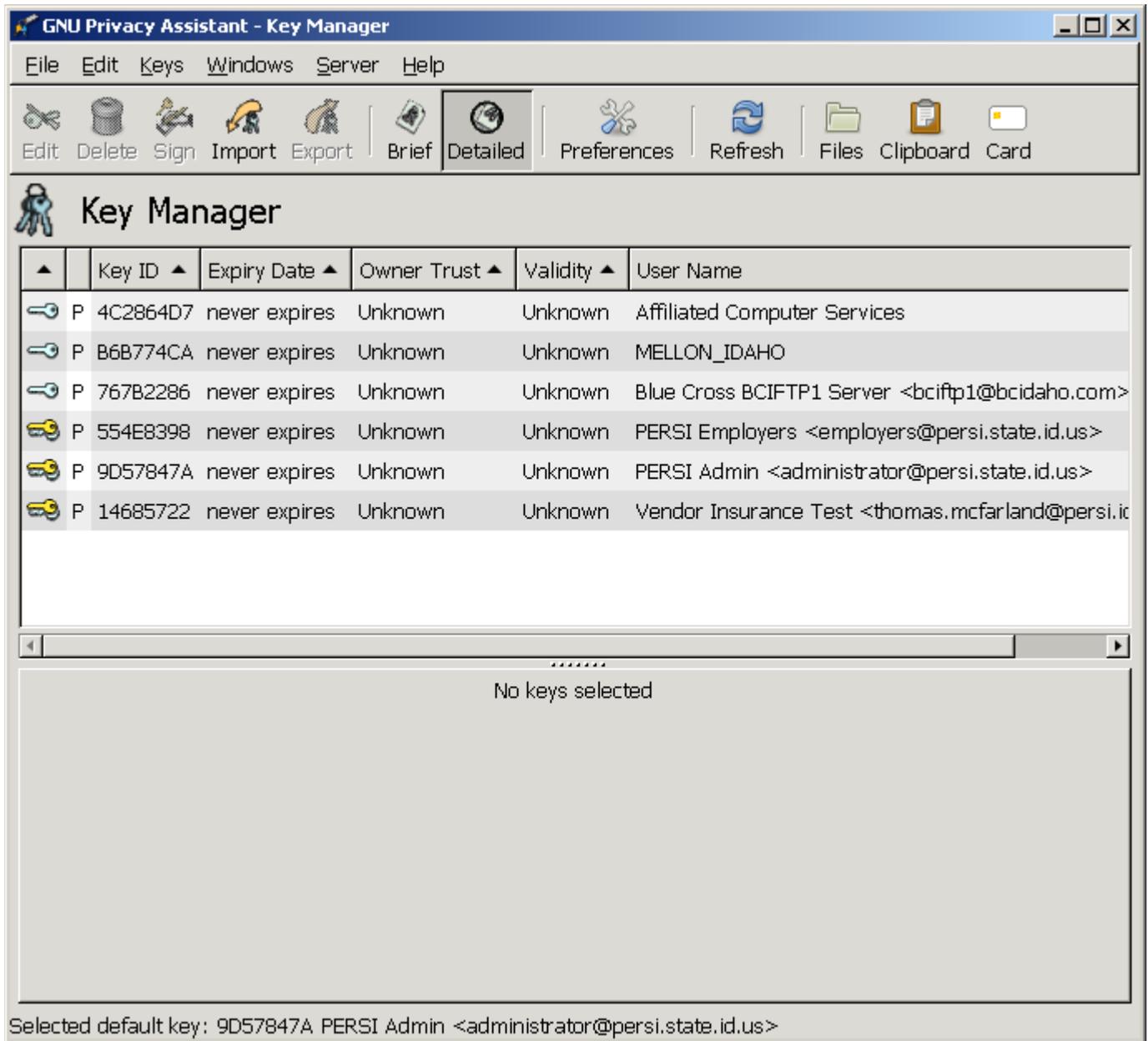
Key ID	User Name
P 4C2864D7	Affiliated Computer Services
P B6B774CA	MELLON_IDAHO
P 767B2286	Blue Cross BCIFTP1 Server <bciftp1@bcidaho.com>
P 554E8398	PERSI Employers <employers@persi.state.id.us>
P 9D57847A	PERSI Admin <administrator@persi.state.id.us>
P 14685722	Vendor Insurance Test <thomas.mcfarland@persi.idaho.gov>

.....

No keys selected

No default key selected in the preferences.

D. Click the Detailed icon in the tool bar.

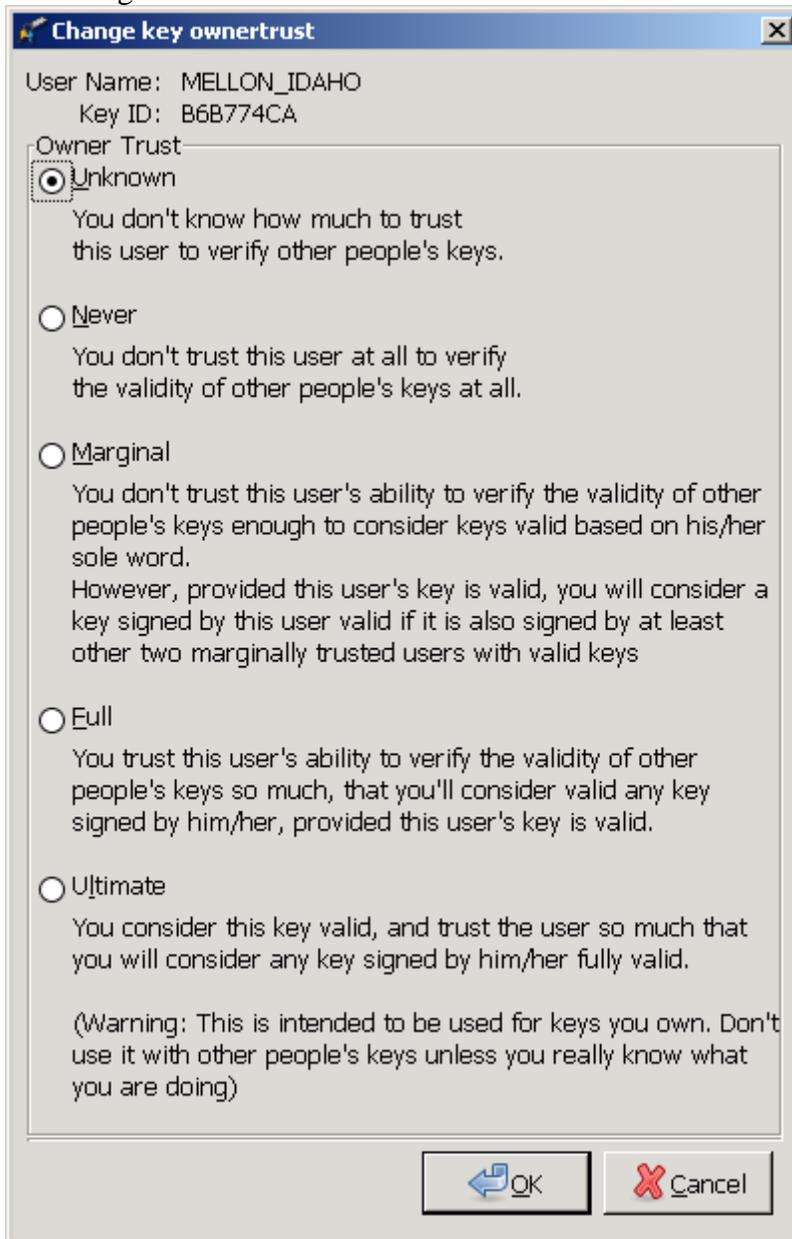


The screenshot shows the GNU Privacy Assistant - Key Manager application window. The title bar reads "GNU Privacy Assistant - Key Manager". The menu bar includes "File", "Edit", "Keys", "Windows", "Server", and "Help". The toolbar contains icons for "Edit", "Delete", "Sign", "Import", "Export", "Brief", "Detailed", "Preferences", "Refresh", "Files", "Clipboard", and "Card". The "Detailed" icon is highlighted. Below the toolbar, the window title is "Key Manager" with a key icon. A table lists several keys with columns for Key ID, Expiry Date, Owner Trust, Validity, and User Name. The table content is as follows:

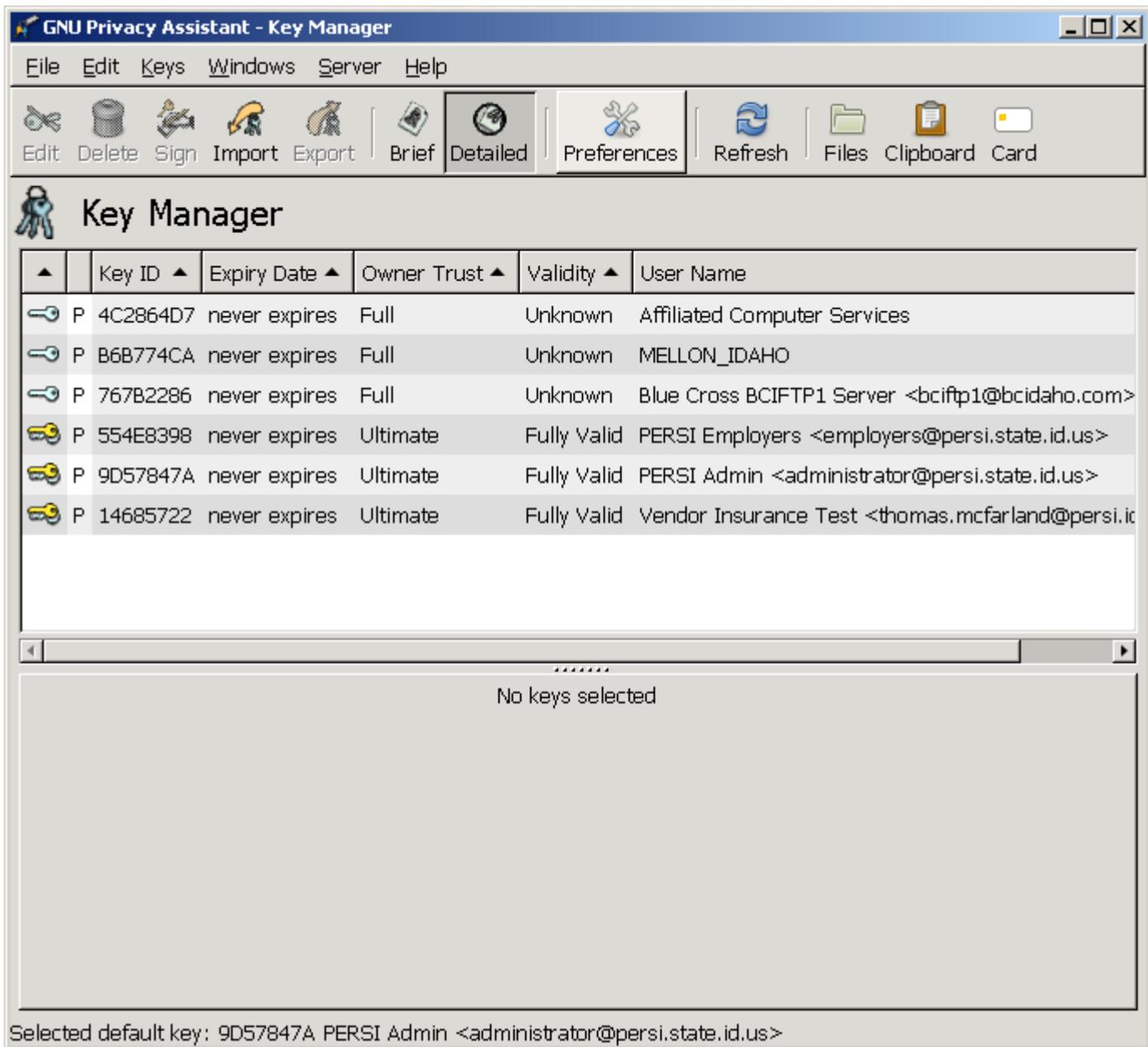
▲	Key ID ▲	Expiry Date ▲	Owner Trust ▲	Validity ▲	User Name
🔑	P 4C2864D7	never expires	Unknown	Unknown	Affiliated Computer Services
🔑	P B6B774CA	never expires	Unknown	Unknown	MELLON_IDAHO
🔑	P 767B2286	never expires	Unknown	Unknown	Blue Cross BCIFTP1 Server <bciftp1@bcidaho.com>
🔑	P 554E8398	never expires	Unknown	Unknown	PERSI Employers <employers@persi.state.id.us>
🔑	P 9D57847A	never expires	Unknown	Unknown	PERSI Admin <administrator@persi.state.id.us>
🔑	P 14685722	never expires	Unknown	Unknown	Vendor Insurance Test <thomas.mcfarland@persi.ic

Below the table, a scroll bar is visible. The main area of the window displays "No keys selected". At the bottom of the window, a status bar reads "Selected default key: 9D57847A PERSI Admin <administrator@persi.state.id.us>".

E. Highlight each key, then use the 'Keys|Set Owner Trust' menu option to display the following dialog.



Set your own keys to 'Ultimate Trust' and others' keys to 'Full'. Click the 'OK' button. Once all of the keys have their trust attribute set, close and restart the GPA application.



- F. Highlight each partner's public key, then use the 'Keys|Sign Keys' menu option to display the following dialog.



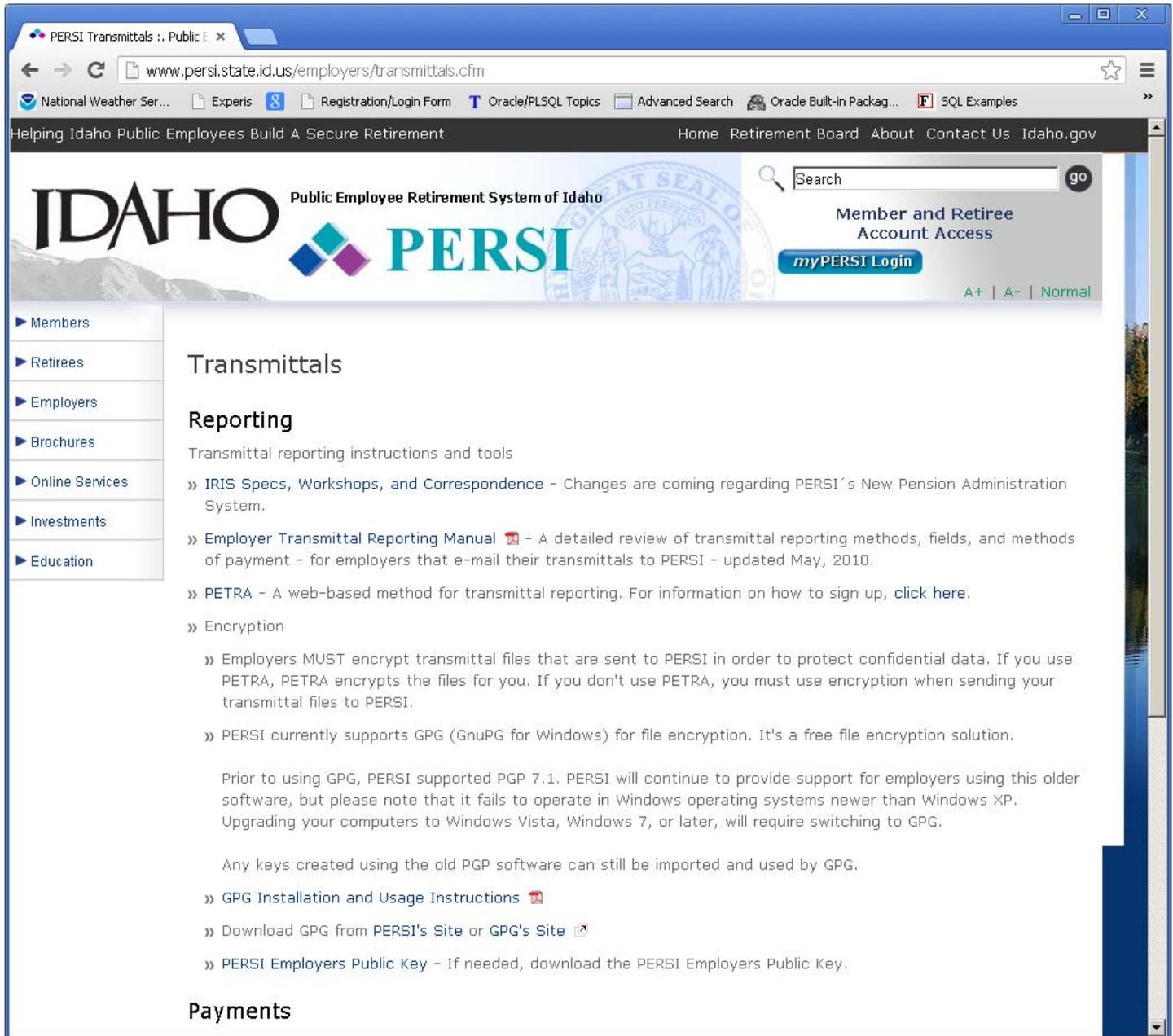
Click 'Yes'. You may have to enter your passkey to sign your partner's public key. Repeat for each public key.

*Key files are created and saved in the c:\Document and Setting\%username\application data\gnupg directory if default file paths were used during installation.

New users only!

12. Download PERSI Public key.

- a. Use your web browser to navigate to the PERSI Employers transmittals page.
<http://www.persi.idaho.gov/employers/transmittals.cfm>



The screenshot shows a web browser window displaying the PERSI Transmittals page. The browser's address bar shows the URL www.persi.state.id.us/employers/transmittals.cfm. The page header includes the Idaho Public Employee Retirement System of Idaho (PERSI) logo and a search bar. A navigation menu on the left lists categories like Members, Retirees, Employers, Brochures, Online Services, Investments, and Education. The main content area is titled 'Transmittals Reporting' and provides instructions and tools for transmittal reporting. It includes several links and sections:

- » IRIS Specs, Workshops, and Correspondence - Changes are coming regarding PERSI's New Pension Administration System.
- » Employer Transmittal Reporting Manual - A detailed review of transmittal reporting methods, fields, and methods of payment - for employers that e-mail their transmittals to PERSI - updated May, 2010.
- » PETRA - A web-based method for transmittal reporting. For information on how to sign up, [click here](#).
- » Encryption
 - » Employers MUST encrypt transmittal files that are sent to PERSI in order to protect confidential data. If you use PETRA, PETRA encrypts the files for you. If you don't use PETRA, you must use encryption when sending your transmittal files to PERSI.
 - » PERSI currently supports GPG (GnuPG for Windows) for file encryption. It's a free file encryption solution.

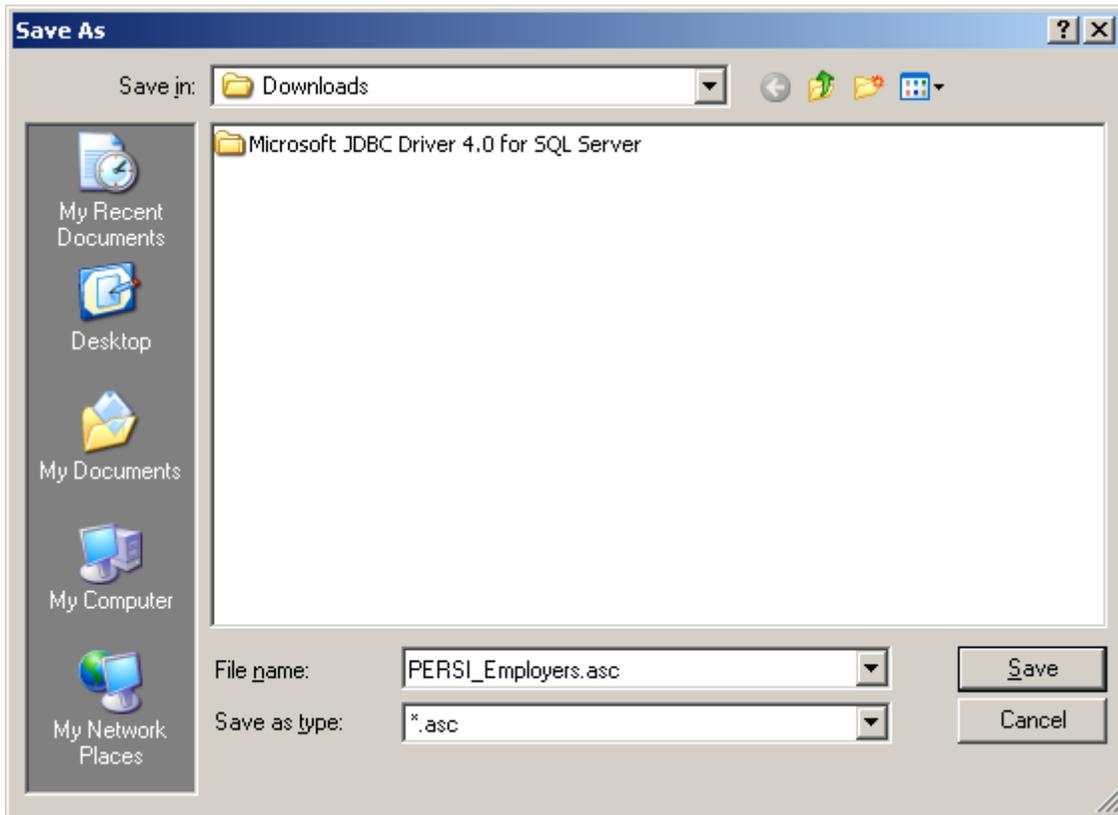
Prior to using GPG, PERSI supported PGP 7.1. PERSI will continue to provide support for employers using this older software, but please note that it fails to operate in Windows operating systems newer than Windows XP. Upgrading your computers to Windows Vista, Windows 7, or later, will require switching to GPG.

Any keys created using the old PGP software can still be imported and used by GPG.

- » [GPG Installation and Usage Instructions](#)
- » [Download GPG from PERSI's Site](#) or [GPG's Site](#)
- » [PERSI Employers Public Key](#) - If needed, download the PERSI Employers Public Key.

The page also has a 'Payments' section at the bottom.

- b. Right click on the “PERSI Employers PGP Public Key” link.
- c. Select the ‘Save link as’ menu option.



D. Click the Save button. Note this directory and filename, as it will be used later.

13. Create your Public/Private Key Pair.

a. Start the GPA application.



b. Click the “Generate key now” button. The following form will display.

Generate key

Generate key

Please insert your full name.

Your name will be part of the new key to make it easier for others to identify keys.

Your Name:

- c. Enter your employer name and click the 'Forward' button.

Generate key

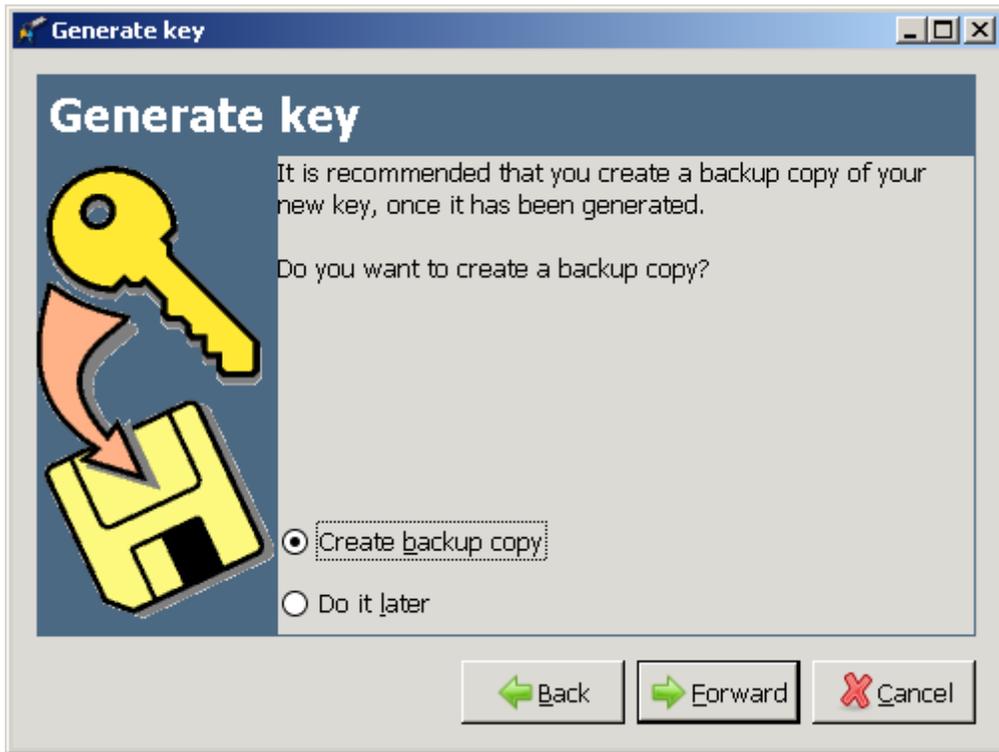
Generate key

Please insert your email address.

Your email address will be part of the new key to make it easier for others to identify keys. If you have several email addresses, you can add further email addresses later.

Your Email Address:

- d. Enter your email address then click the 'Forward' button.



- e. Leave the default selection “Create backup copy” and click the “Forward” button.



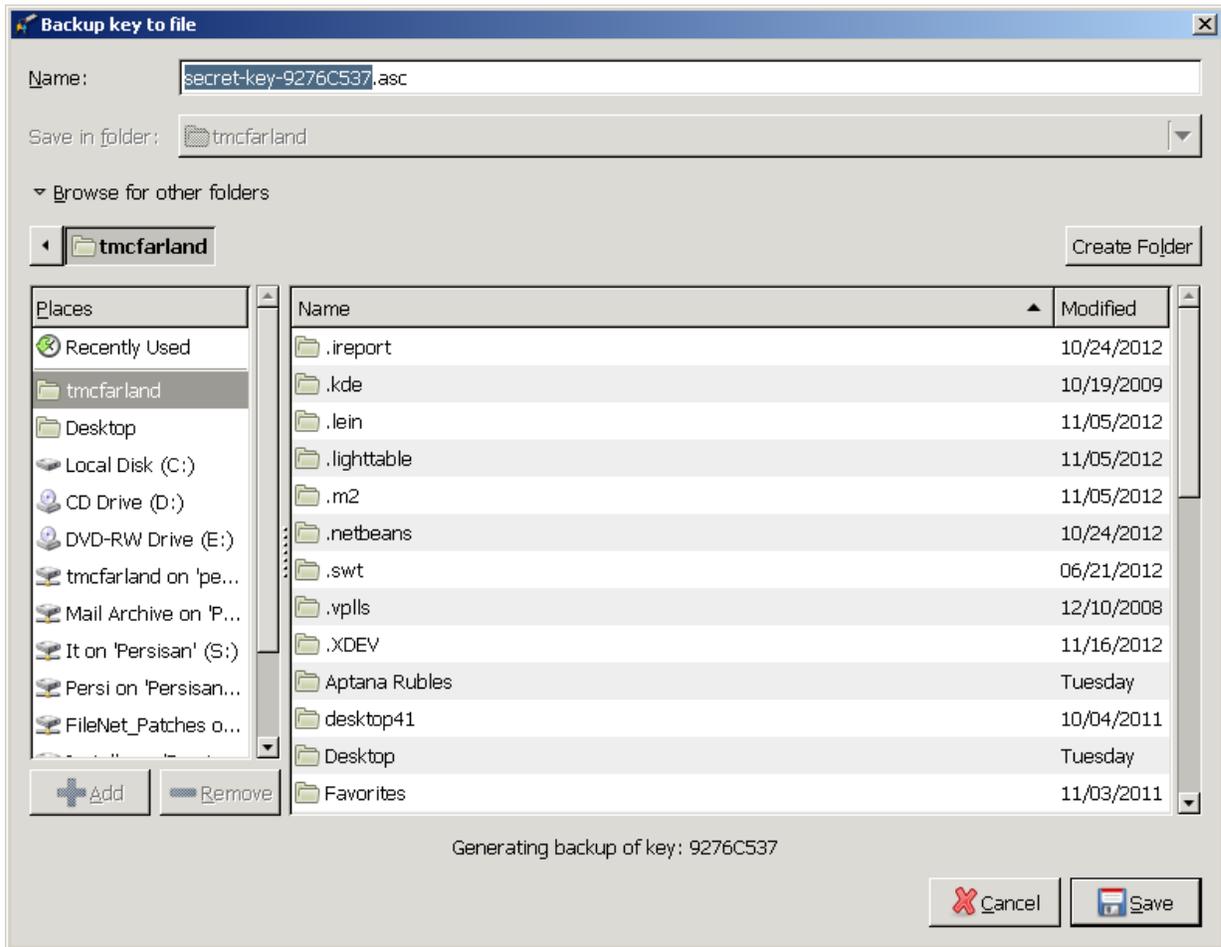
- f. Enter a passphrase (you must use letters and numbers and meet minimum length requirements), then click the “OK” button.

This passphrase is very important and your key pair cannot be used without it.

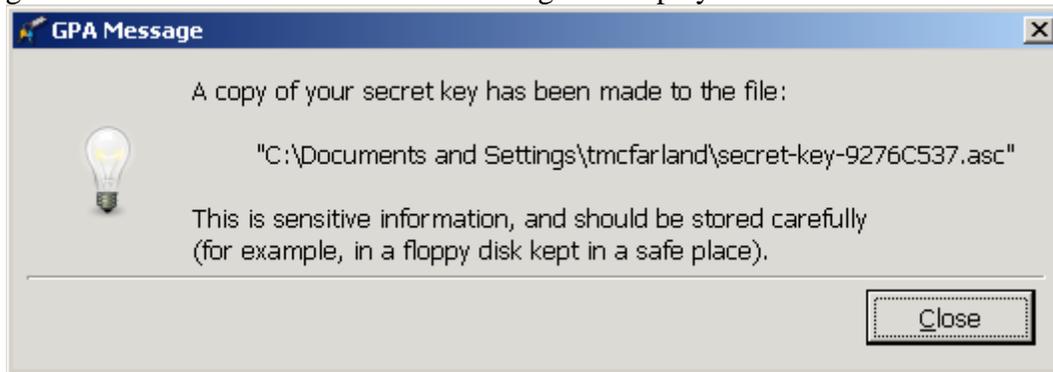
Keep it in a secure place.



Re-enter your passphrase. If you successfully reproduce your passphrase the next display will appear.



g. Click the “Save” button. The following will display.



- h. Click the “Close” button. The 2.1.0 version of the software can end your gpa.exe program with an error. If you receive the ‘Please tell Microsoft about this problem’ dialog, just click the ‘Don’t Send’ button. Then, double click the GPA icon to restart the program.
- i. Your key pair should be displayed.

GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

Edit Delete Sign Import Export Brief Detailed Preferences Refresh Files Clipboard Card

Key Manager

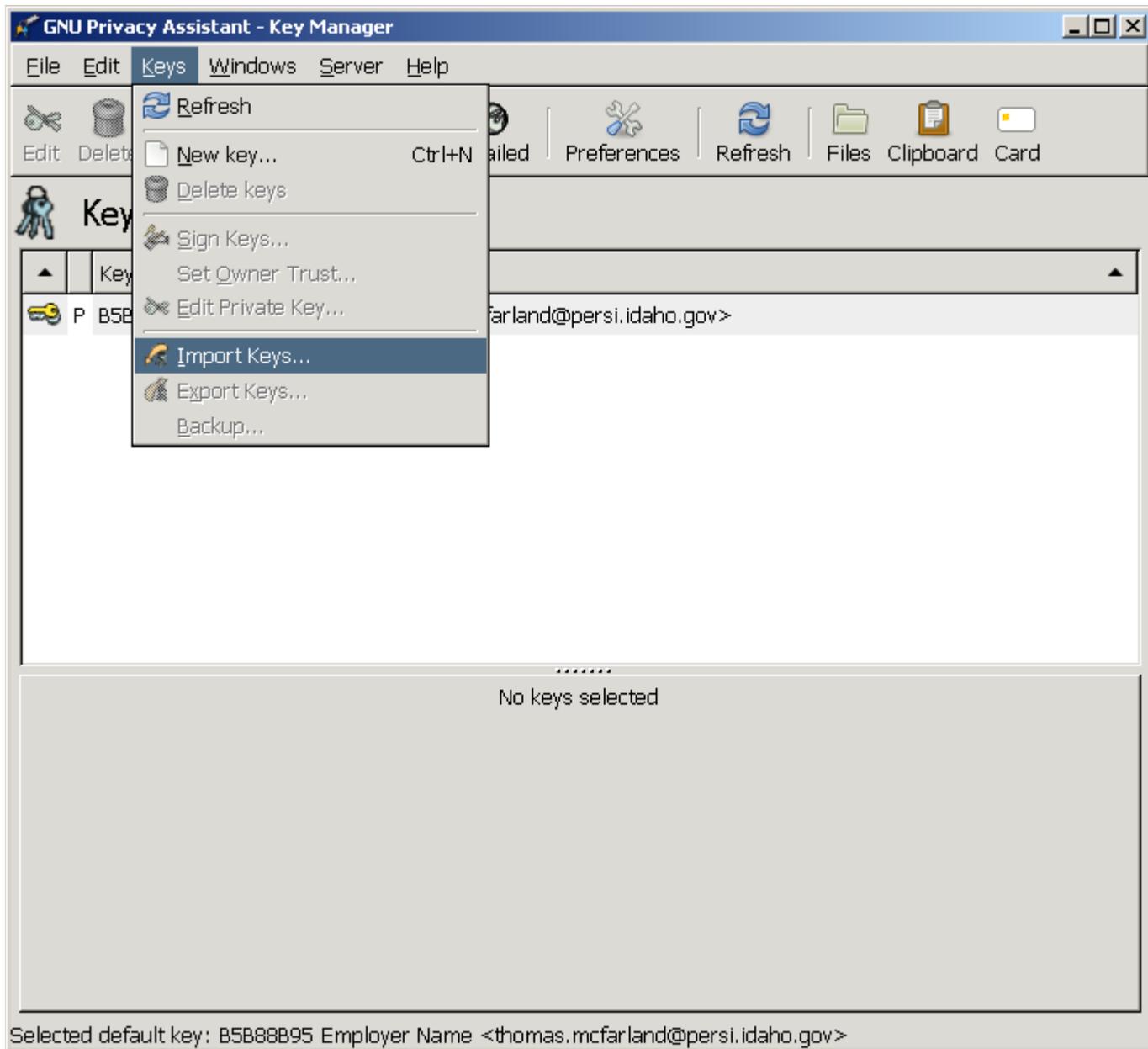
▲	Key ID ▲	User Name ▲
	P B5B88B95	Employer Name <thomas.mcfarland@persi.idaho.gov>

.....

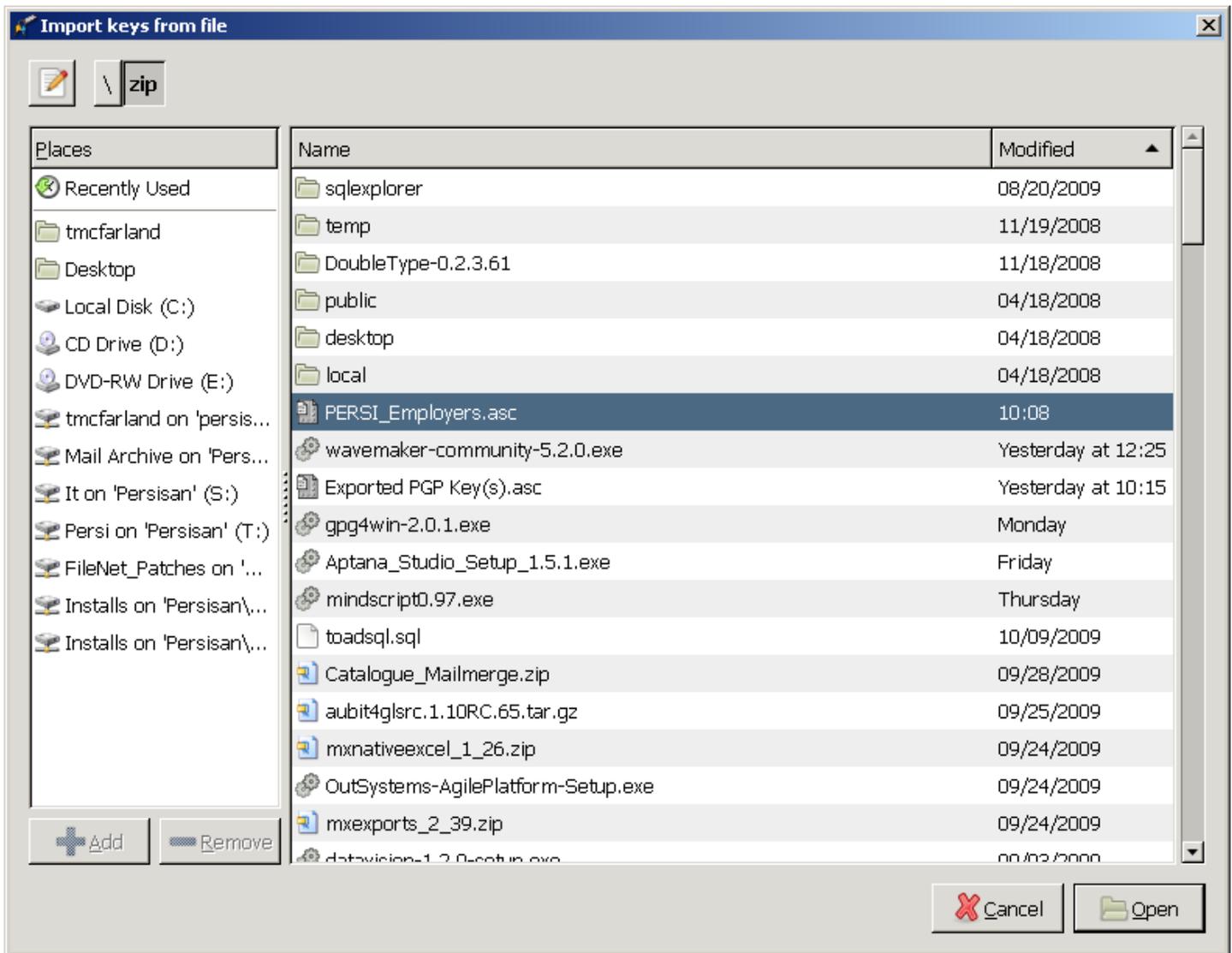
No keys selected

Selected default key: B5B88B95 Employer Name <thomas.mcfarland@persi.idaho.gov>

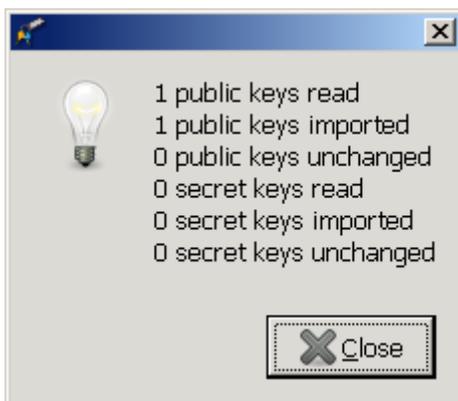
14. Import the PERSI public key into gpg4win.
 - a. Select the menu action Keys|Import .



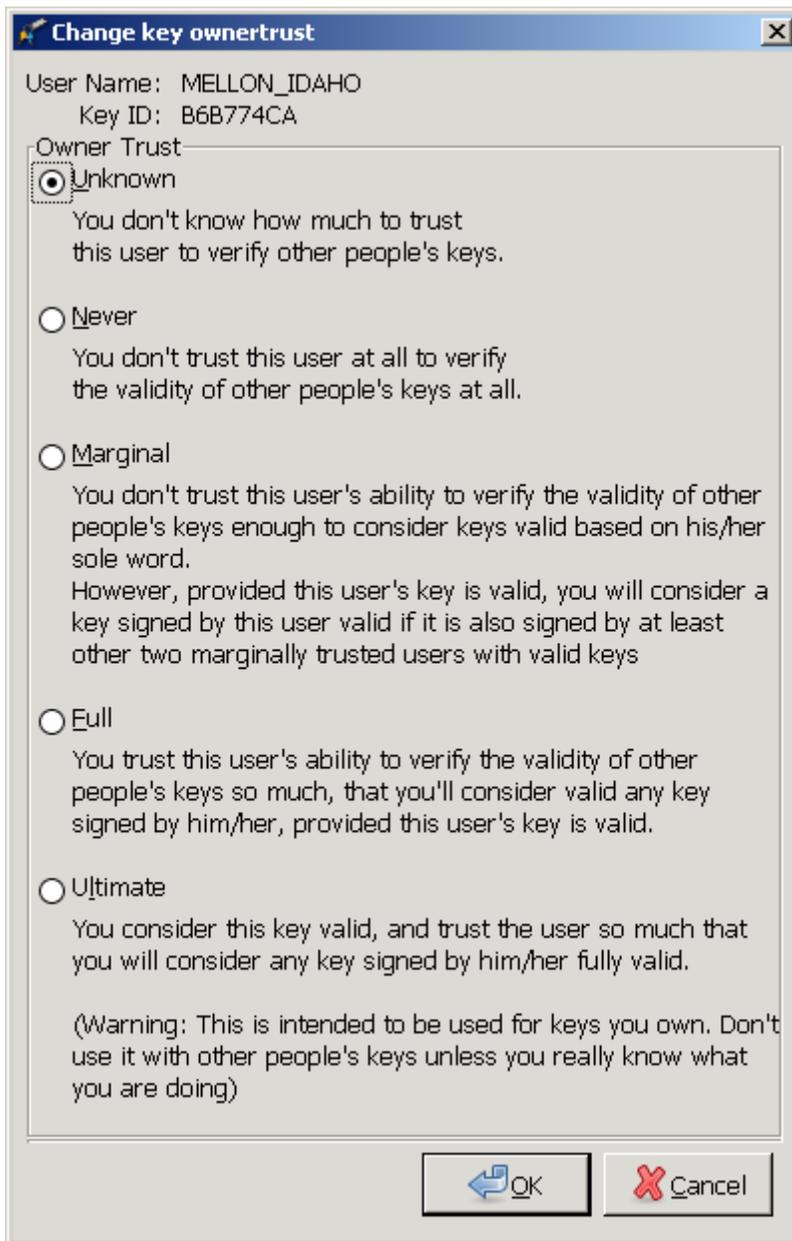
A file dialog box will be opened.



- b. Navigate and find the PERSI_EMPLOYERS.asc file that you previously downloaded. Click the “Open” button.



- C. Click the “Close” button.
 D. Highlight each key, then use the ‘Keys|Set Owner Trust’ menu option to display the following dialog.

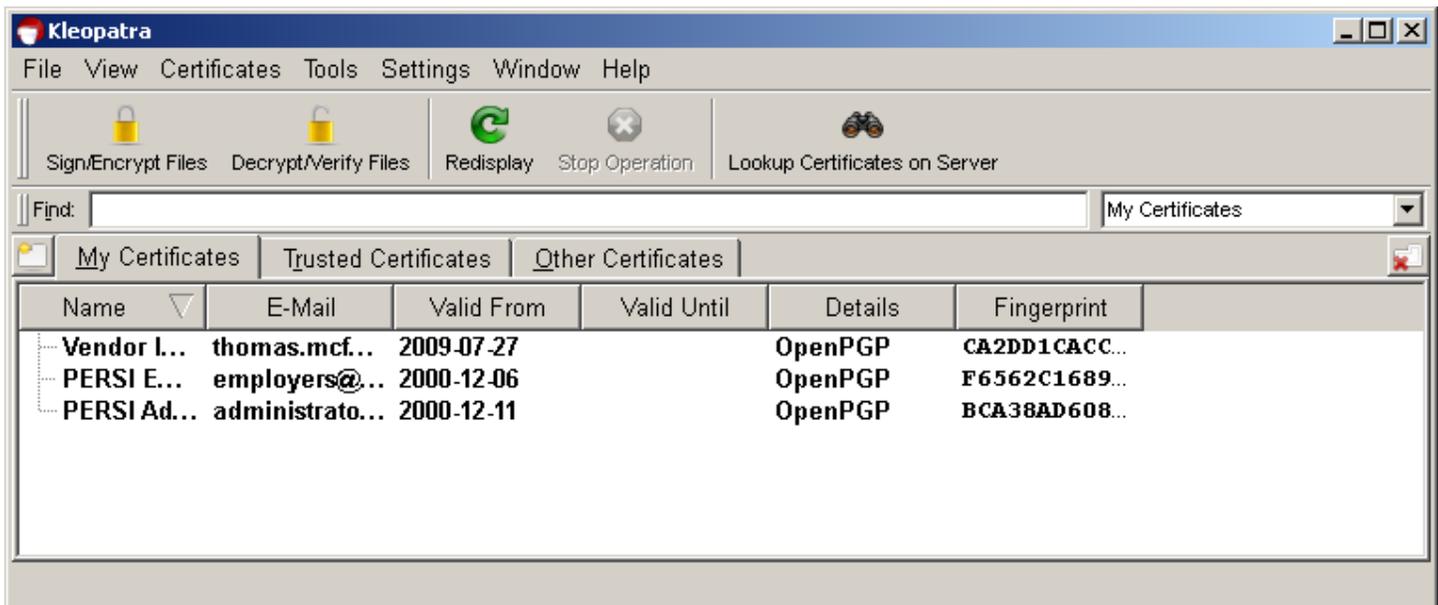


Set your own keys to 'Ultimate Trust' and other's keys to 'Full'. Click the 'OK' button. Once all of the key have their trust attribute set, close and restart the GPA application.

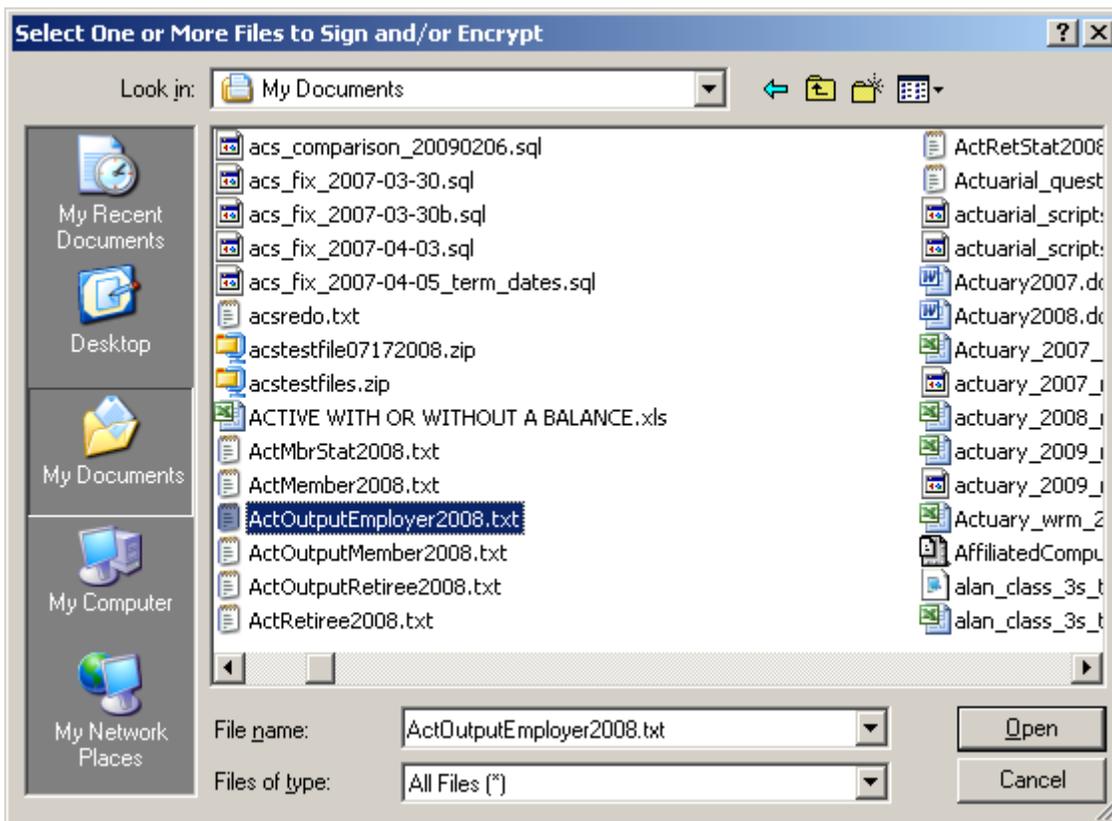
E. You are Done! Close the GPA application.

Encrypting and Signing Instructions

1. Start the Kleopatra application.

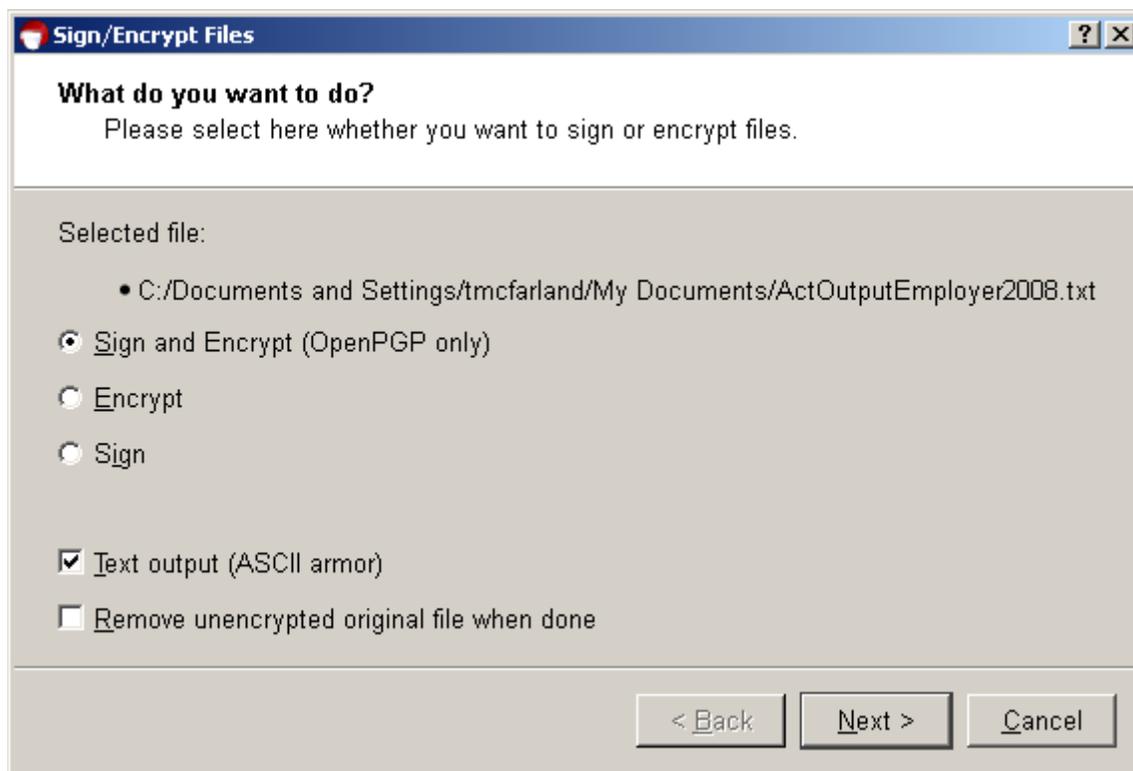


2. Click the Sign/Encrypt Files icon (also available from the File menu).



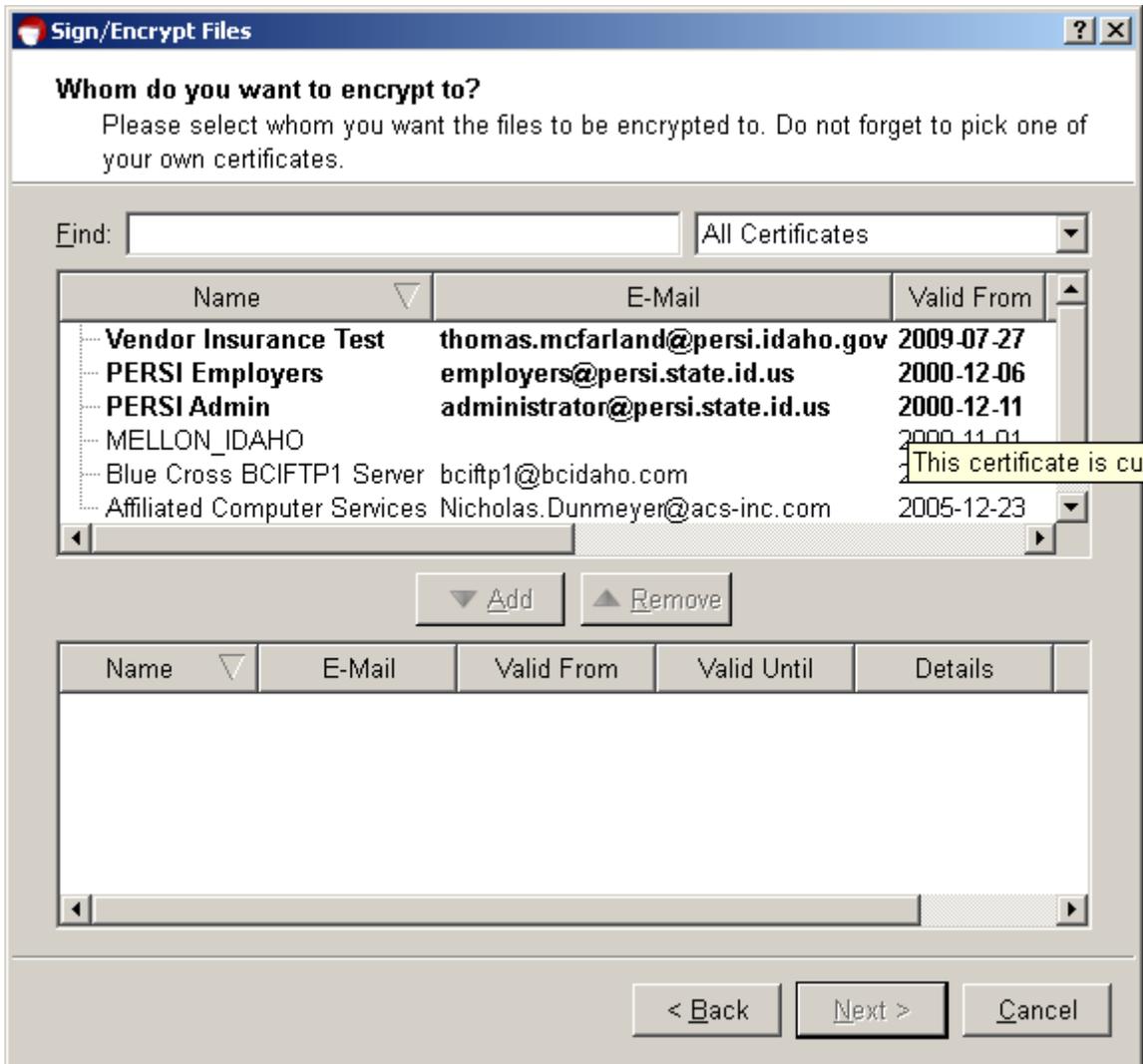
3. Navigate to find the file you want to encrypt and click the 'Open' button.

4. Choose your encryption options.

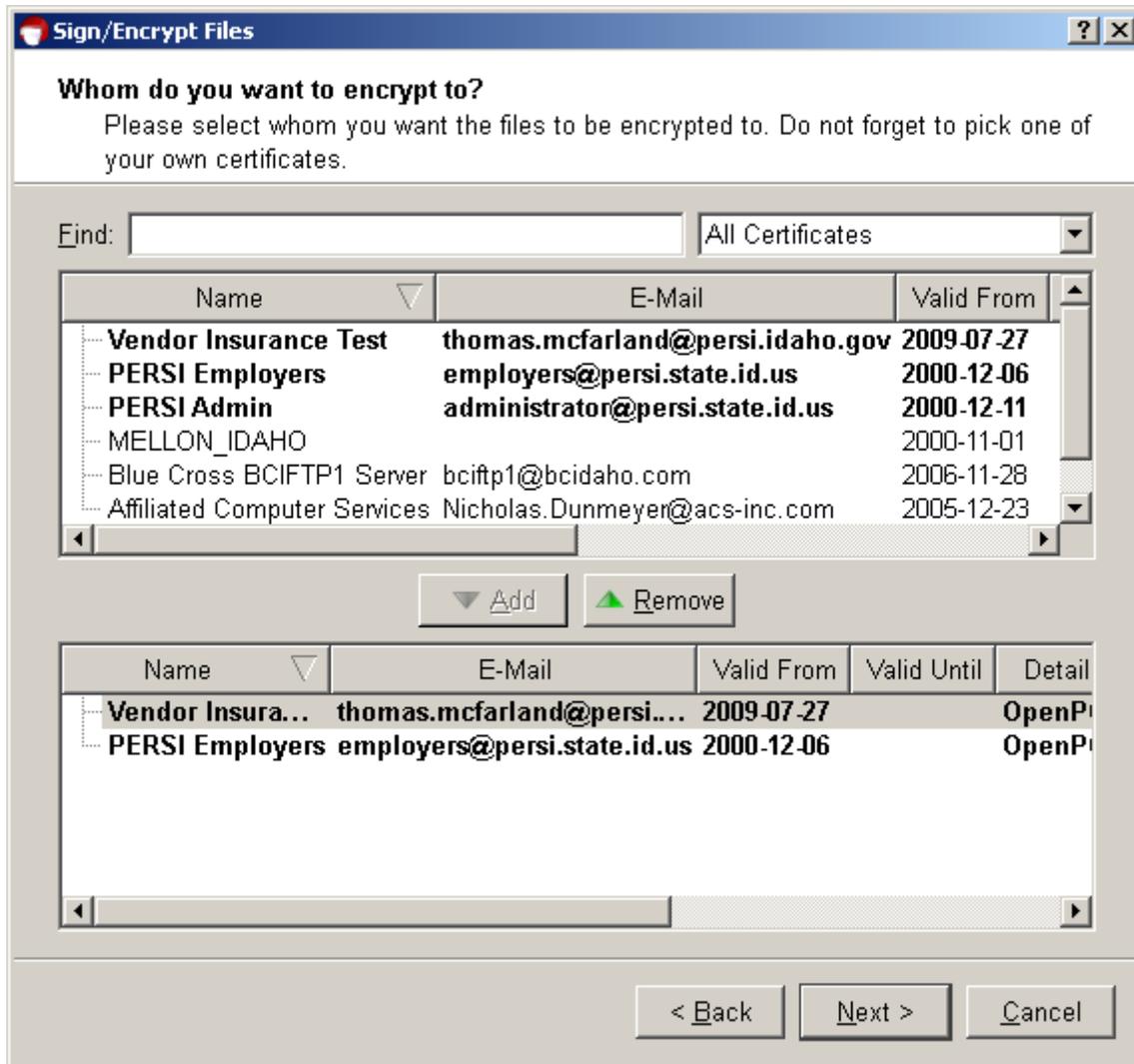


A. Click “Next”. If ‘Text output (ASCII armor)’ is unchecked the file will encrypt but have a .gpg extension.

5. Select the recipients for the file.

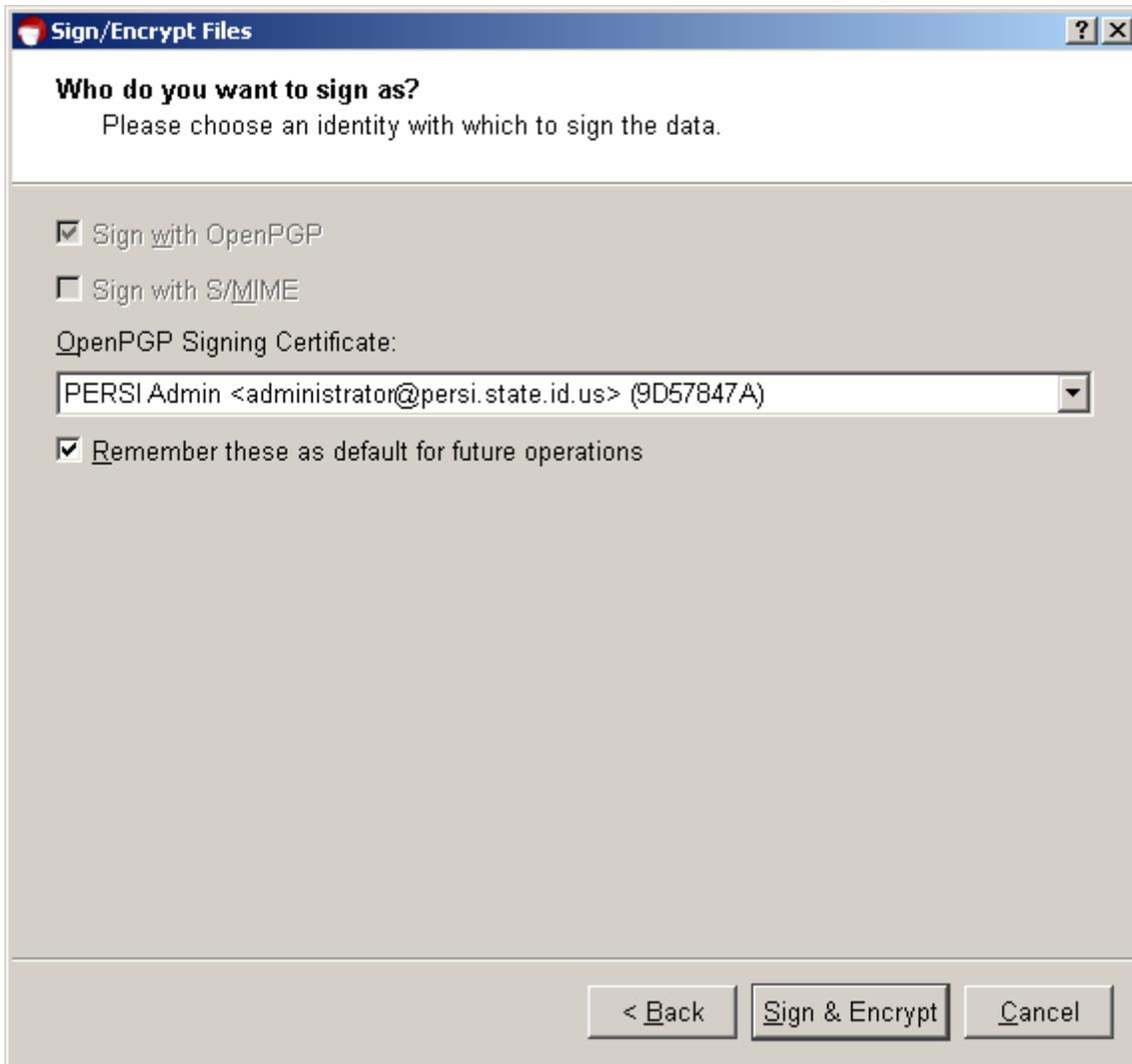


6. Highlight the recipient name(s) (including yourself and PERSI) and click the add button.



A. Click the "Next" button.

7. Choose the signing key.



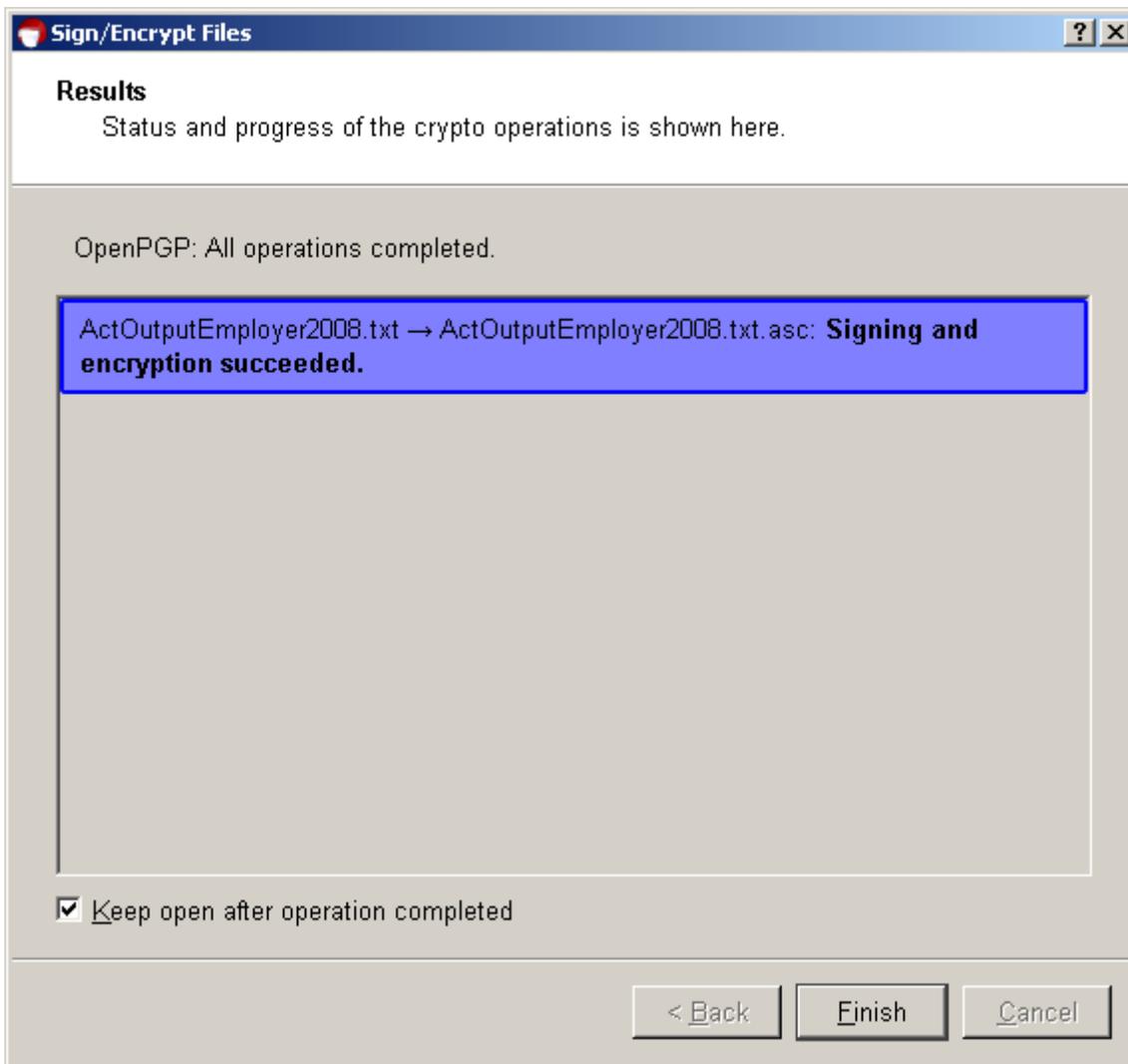
A. Click the Sign & Encrypt button.

8. Enter the Pass Phase.



A. Click "OK".

9. View the results screen.

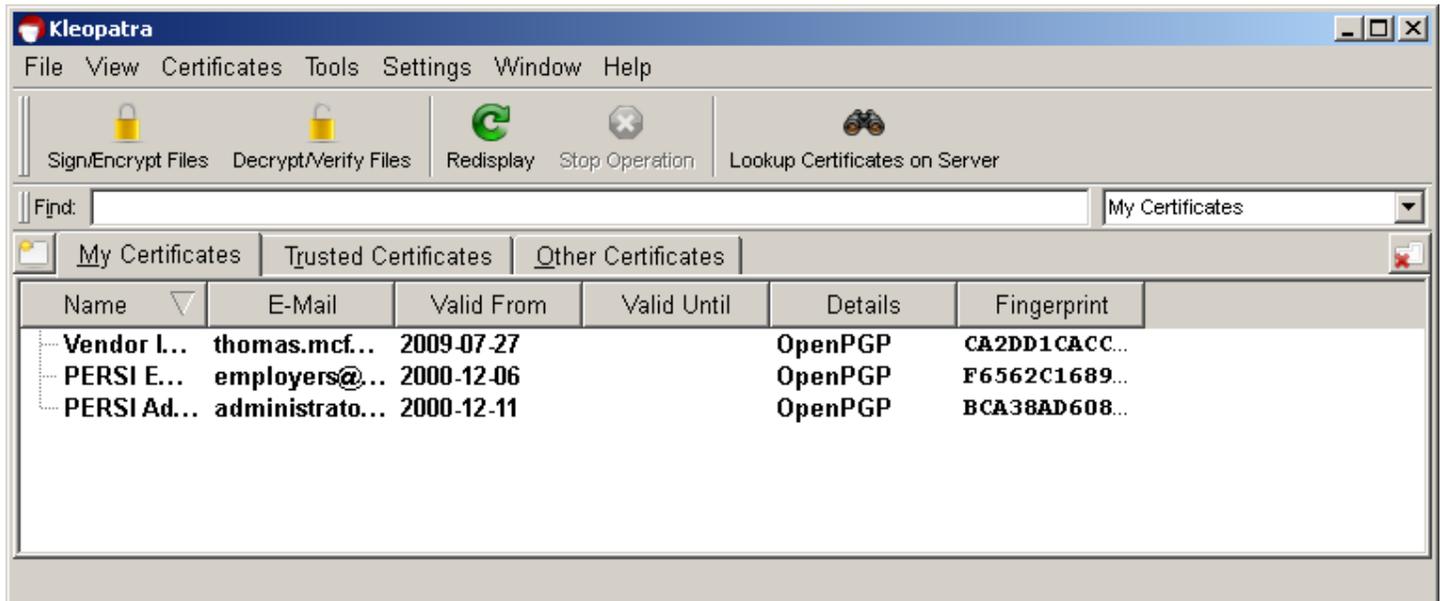


A. Click "Finish".

Note: The export file will now be compressed (to approx. 10% of original size), encrypted and copied to a new file of the same name with the added extension of .asc or pgp.

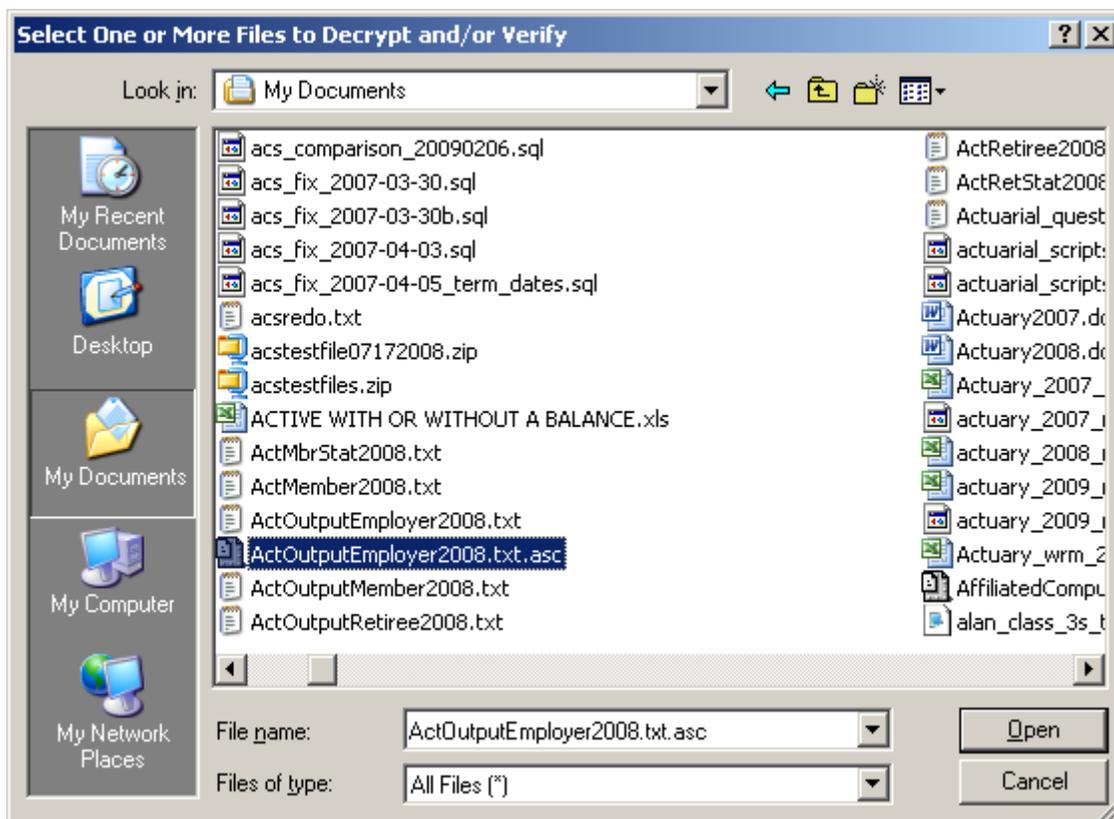
Decrypting Instructions

1. Start the Kleopatra application.



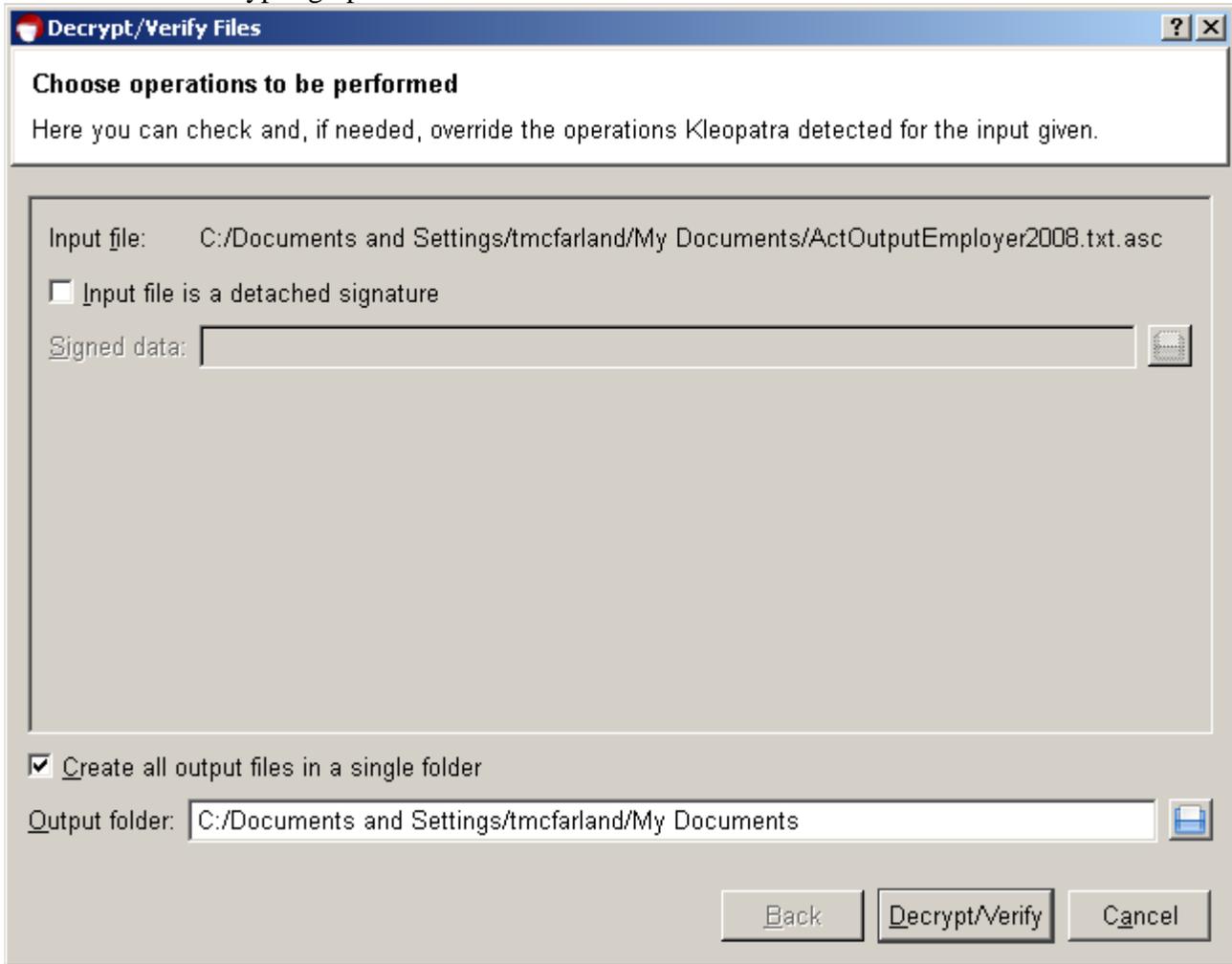
A. Click the Decrypt/Verify Files icon.

2. Navigate and select the file to decrypt.



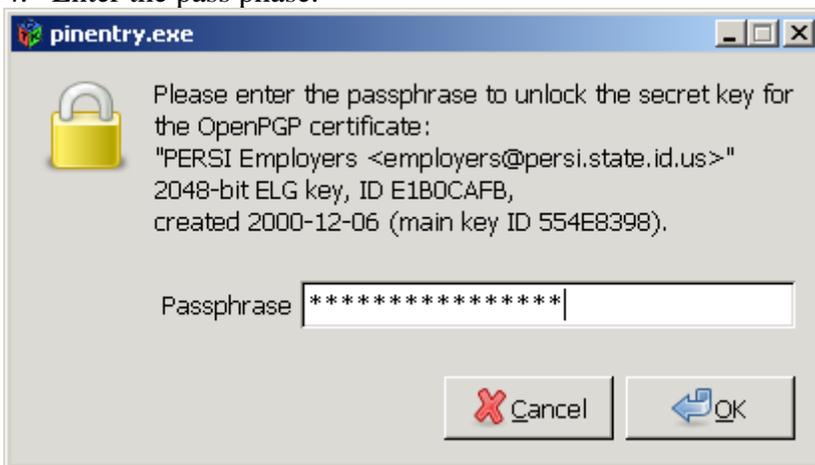
A. Click the Open button.

3. Choose the decrypting options.



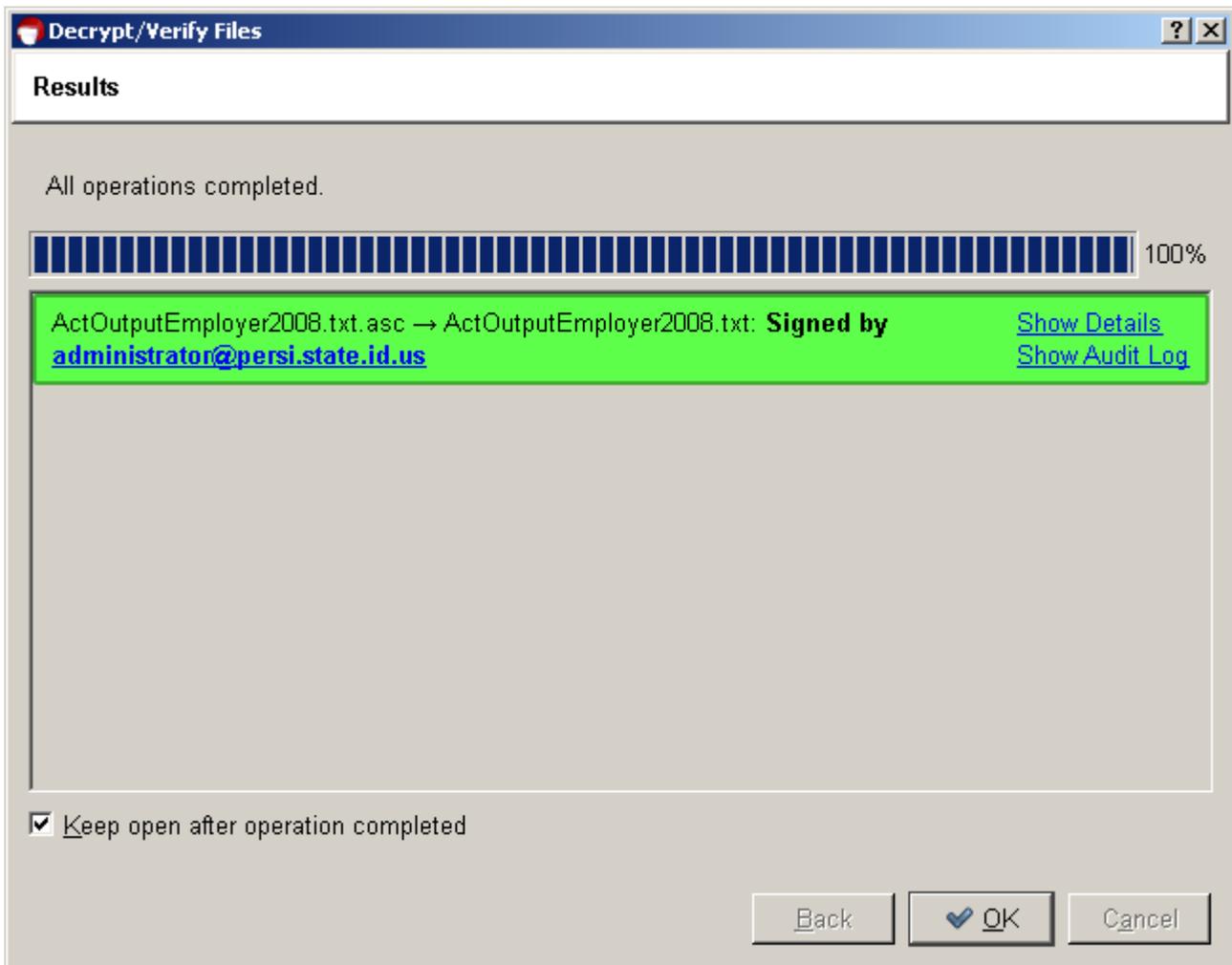
A. Click the Decrypt/Verify button.

4. Enter the pass phase.



A. Click the OK button.

5. View Results screen.



A. Click the OK button.

Transmitting (Uploading) the File to PERSI

1. Within Outlook / Outlook Express (or other email client) create a new mail message as follows:

To: employers@persi.idaho.gov

Subject: **M545_Biweekly_20091130.xmt.asc** (Subject must be the same as export file name)

2. **Insert** the newly encrypted file as an attachment.

3. Click on **Send**. You're Done!

Command Line Scripting

If you are using the command line interface the command line scripts will need updated.

Examples.

Current encryption command

```
pgp -sea filepath\filename "Send to Company Name" -u "from signing key" -z passphrase1
```

New encryption command

```
gpg --batch -u "from signing key" --passphrase passphrase1 -sea -r "Send to Company Name" filepath\filename
```

Current decryption command

```
pgp +batchmode +force "filepath\filename" " " -u "recipient_key" -z passphrase
```

New decryption command

```
gpg --batch -o "outputfilepath\filename" -r "recipient" --passphrase "passphrase1" --decrypt  
"filepath\filename.gpg"
```

* any file paths, file names or user names with embedded spaces must be enclosed in double quotes