



PERSI EMPLOYER TRANSMITTAL PROCEDURE

Each of the 500+ PERSI Employers 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). 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

1. Download software from web site. <http://www.gpg4win.org/download.html>
(current version as of 10/31/2009 was 2.0.1)
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.



- A. The software is not digitally signed. Click on the 'Run' button.

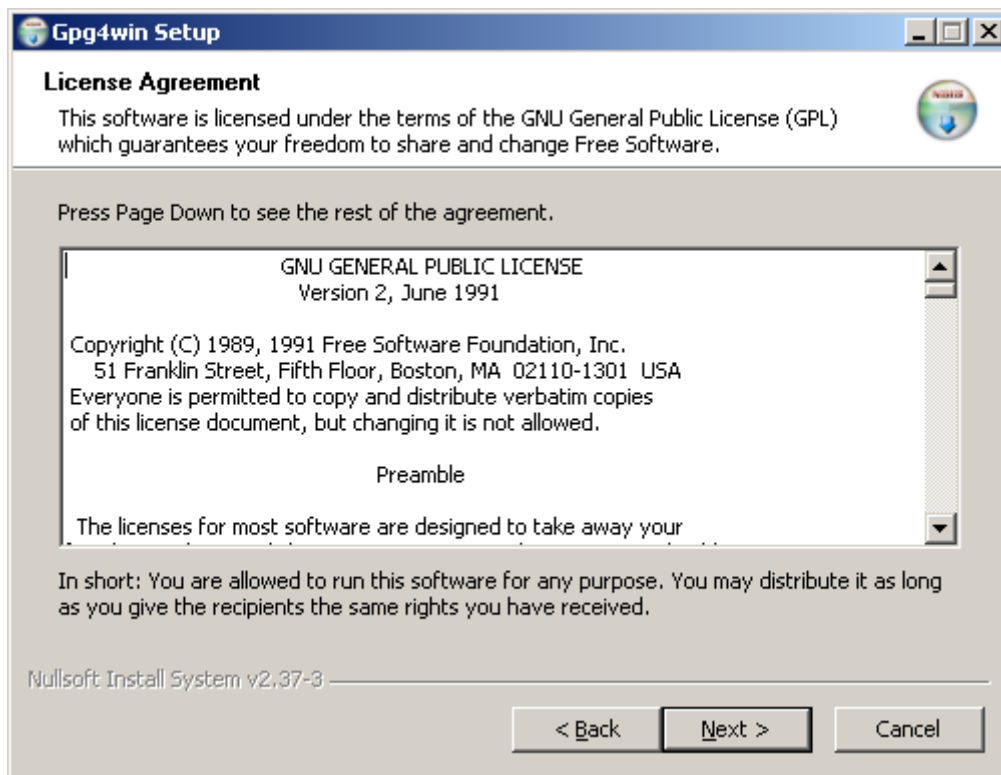


- B. Select the install language and Click 'OK'.



A. Click Next.

4. Accept the license.



A. Click Next.

5. Choose following software modules for installation.

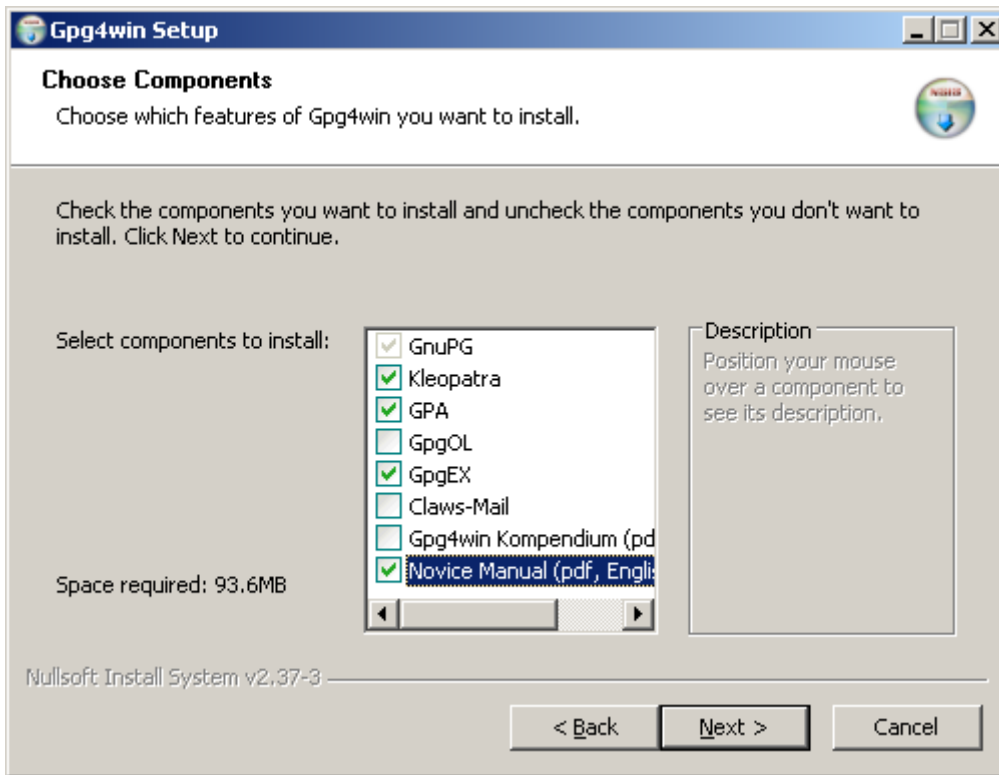
GnuPG

Kleopatra (replacement for PGPTools)

GPA (key manager)

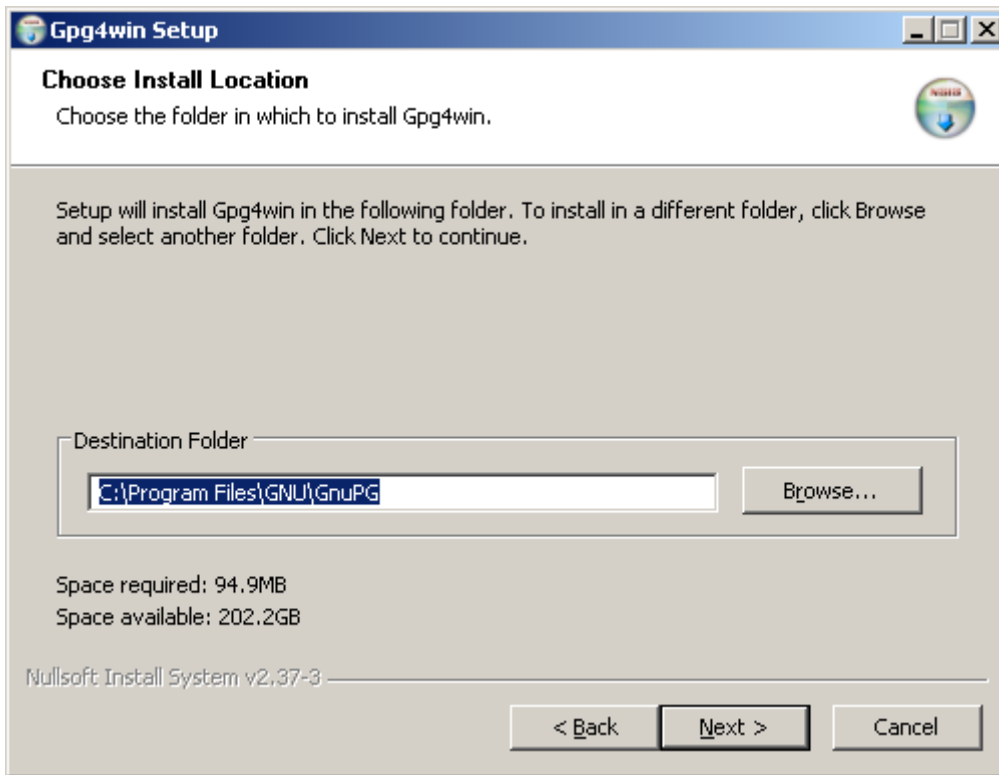
GpgEx

Novice Manual



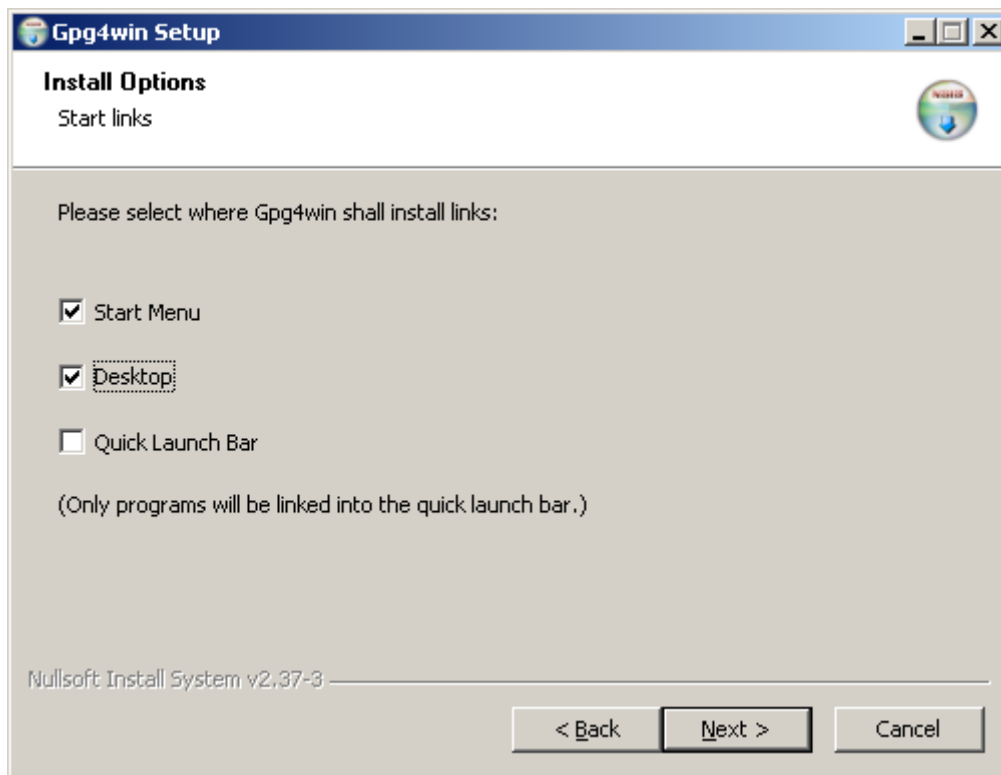
A. Click Next.

6. Enter or accept the installation path.



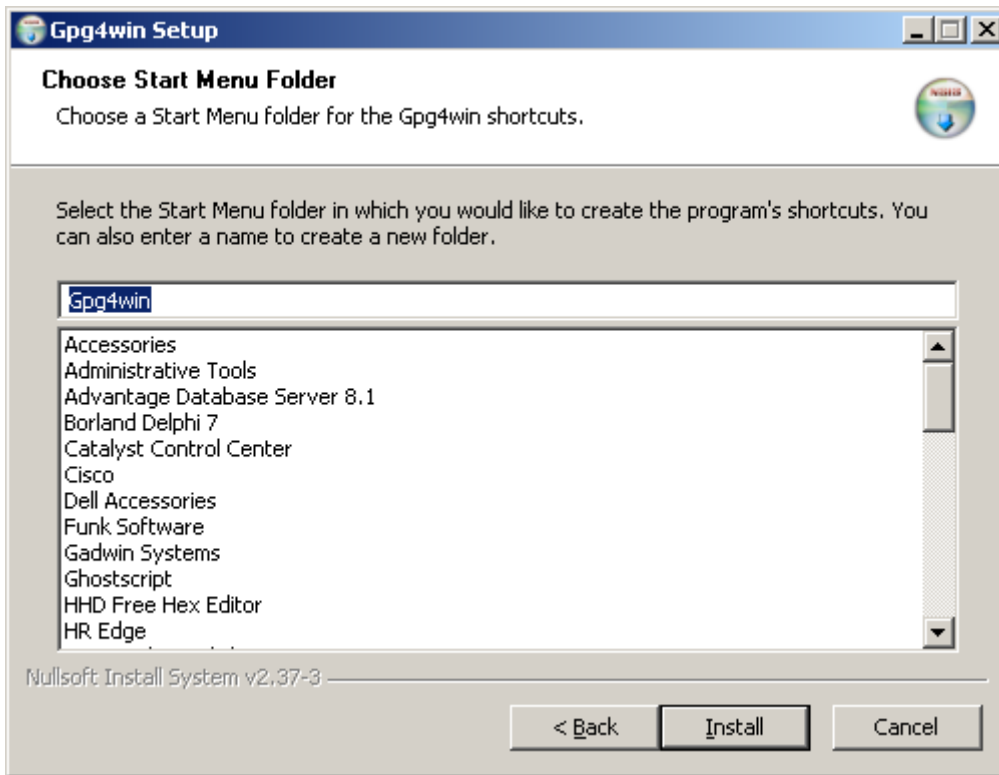
A. Click Next.

7. Choose the installation options.



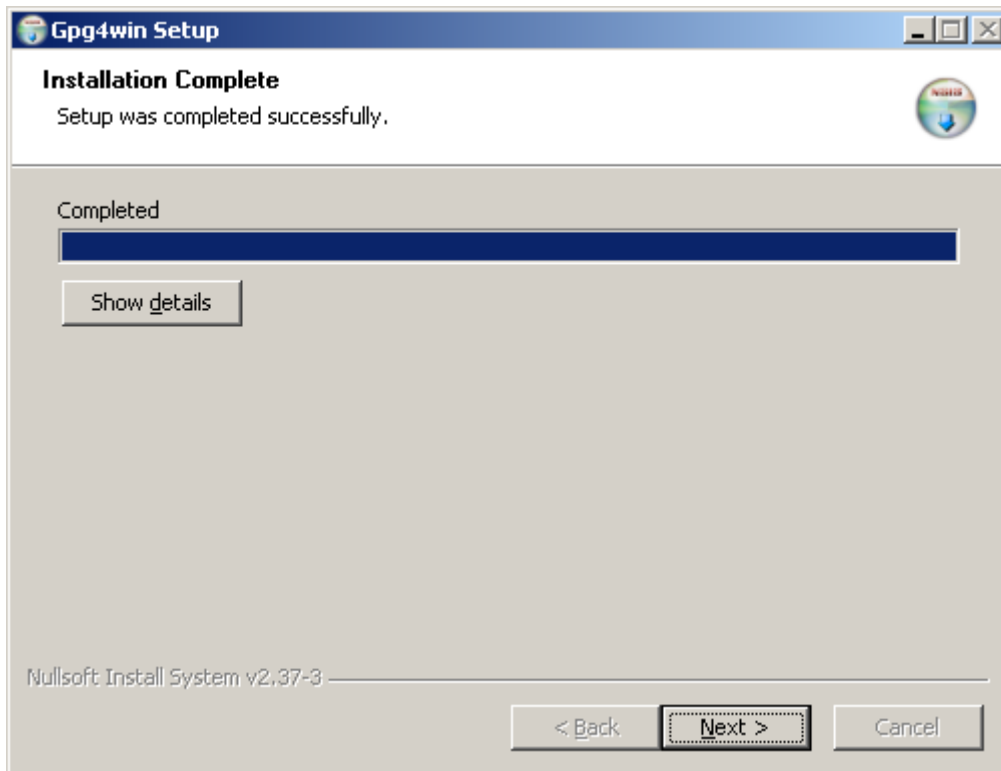
A. Click Next.

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.

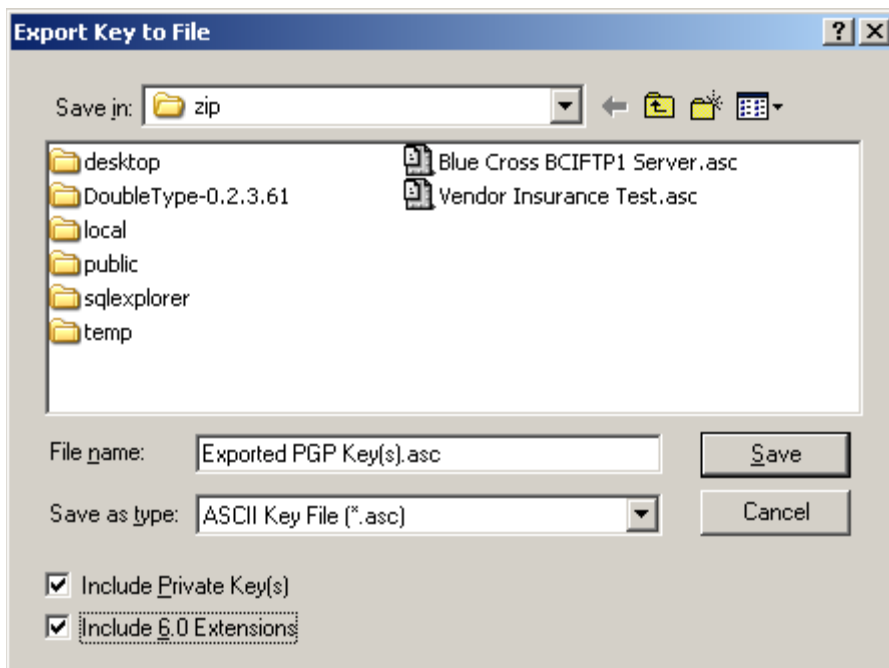
9. You may need to reboot your system depending on what is currently running while the installation takes place.



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

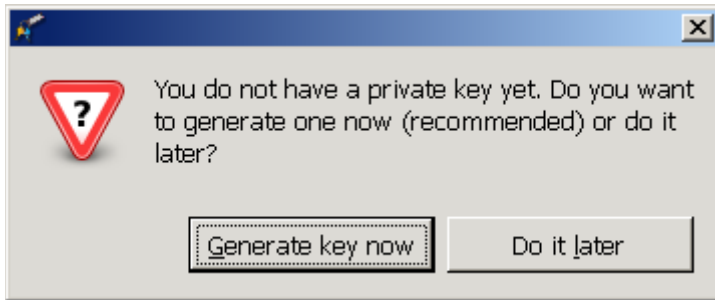
Existing PGP Users: If you are converting from PGP to gpg4win continue; otherwise skip to step 12.
New Users: Proceed to step 12.

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



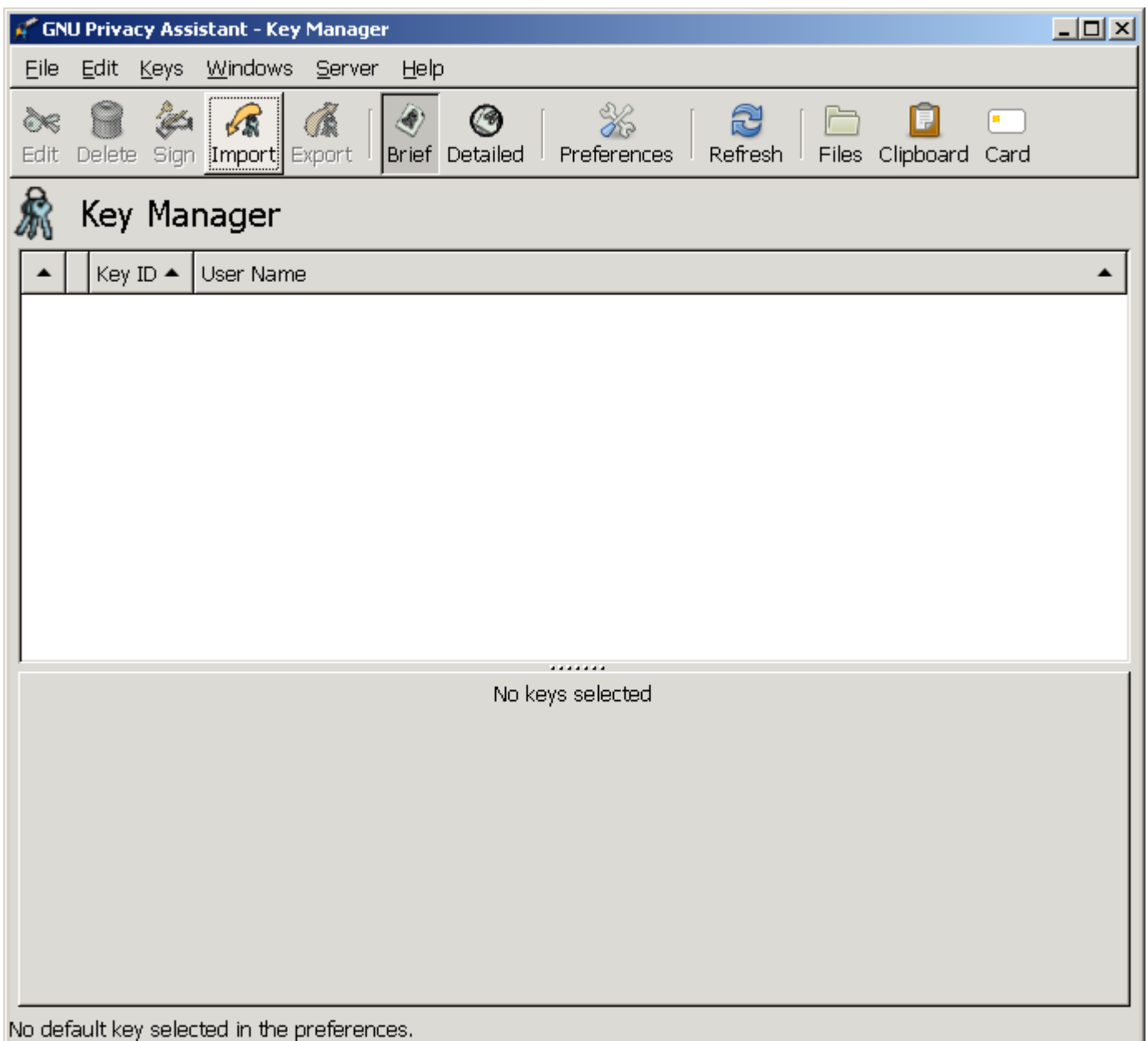
- D. Enter the File name.
- E. Check the include Private Key(s), and include 6.0 extensions check boxes.
- F. Click the Save button.

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

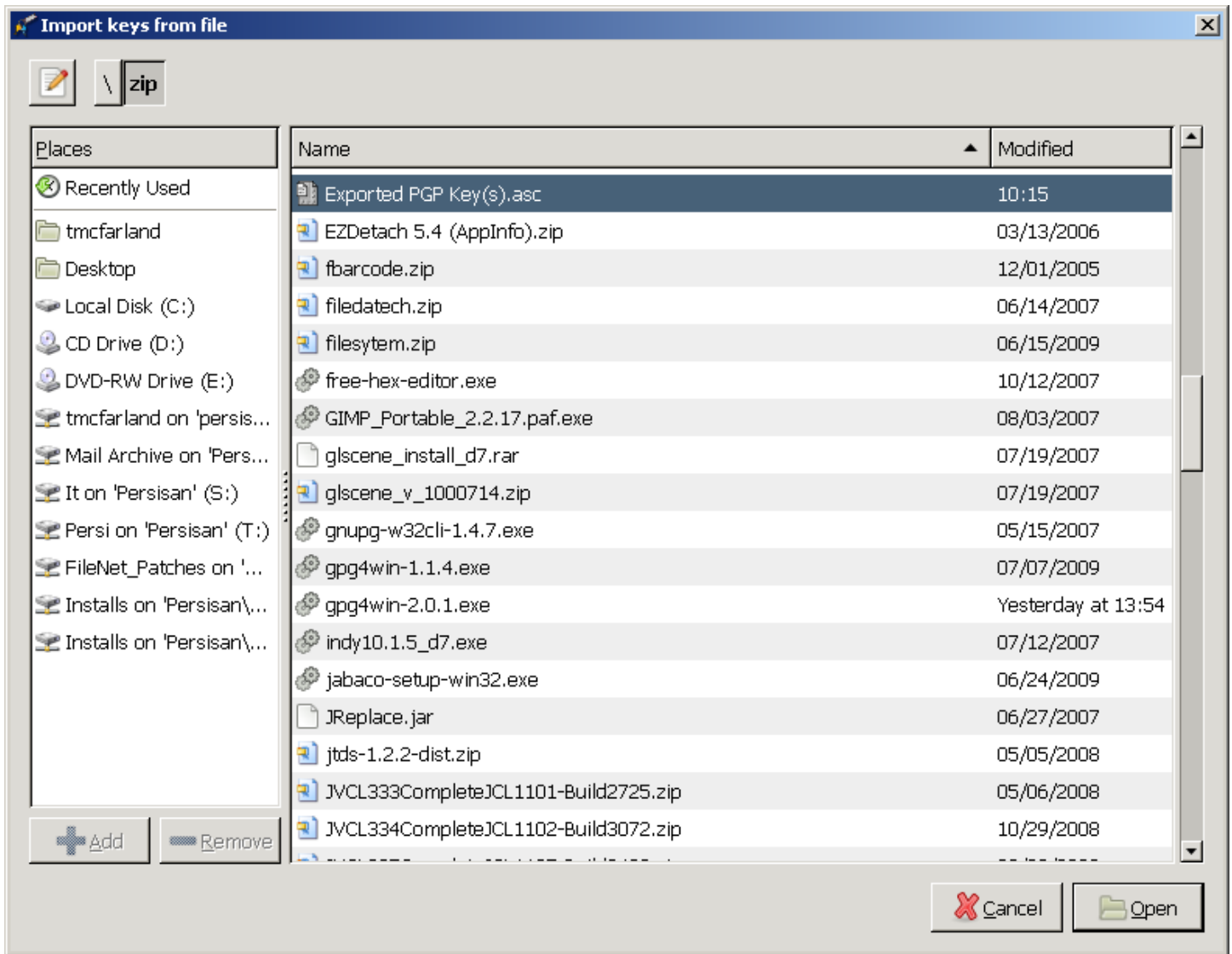


A. Click the “Do it Later” button.

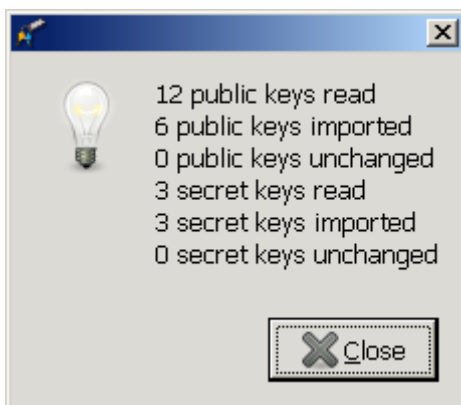
The GPA application will be displayed.



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

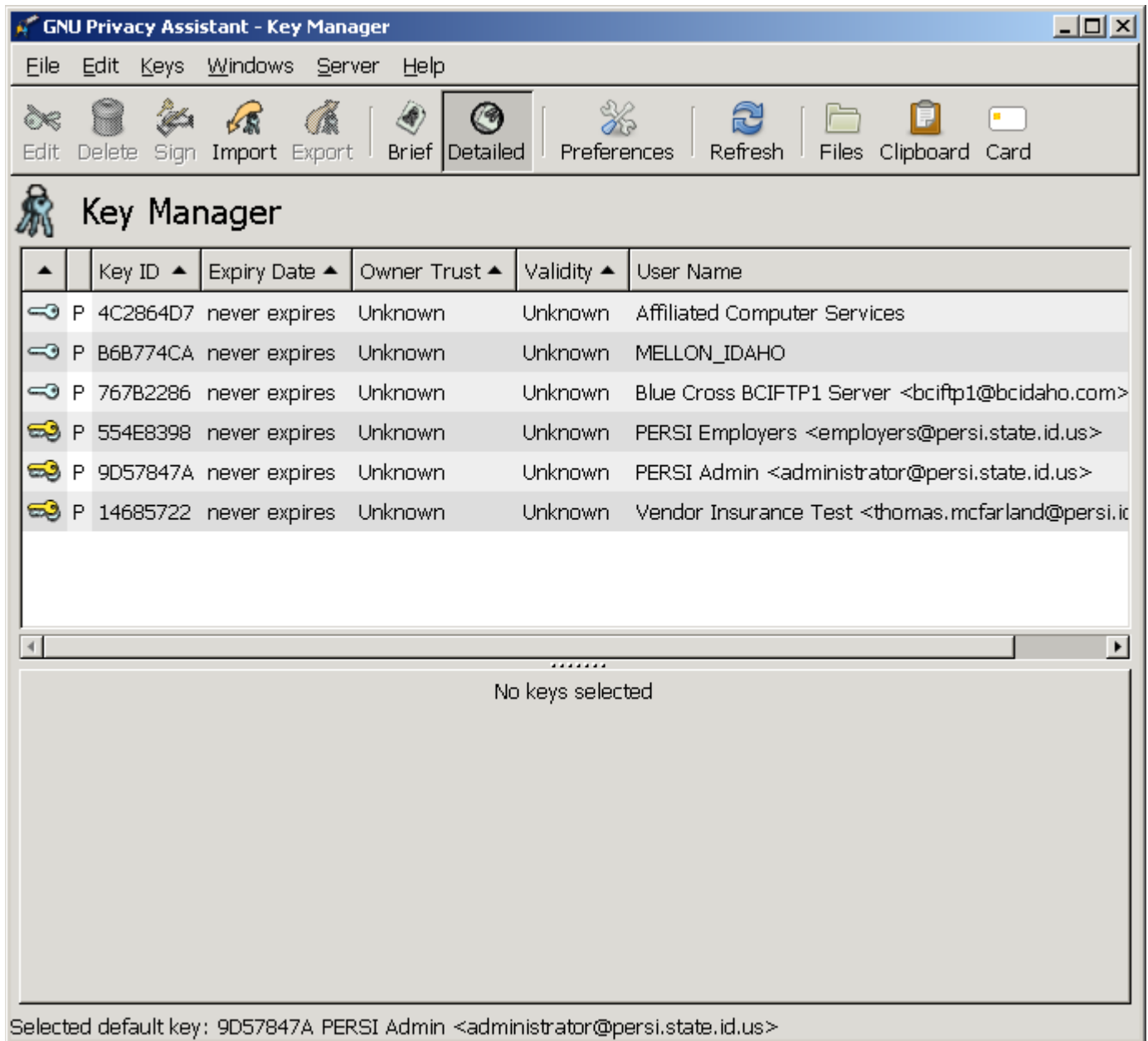
Key ID	User Name
P 4C2864D7	Affiliated Computer Services
P B6B774CA	MELLON_IDAHO
P 767B2286	Blue Cross BCIFTP1 Server <bciftp1@bcidaho.com>
P 554E8398	PERSI Employers <employers@persi.state.id.us>
P 9D57847A	PERSI Admin <administrator@persi.state.id.us>
P 14685722	Vendor Insurance Test <thomas.mcfarland@persi.idaho.gov>

.....

No keys selected

No default key selected in the preferences.

D. Click the Detailed icon in the tool bar.

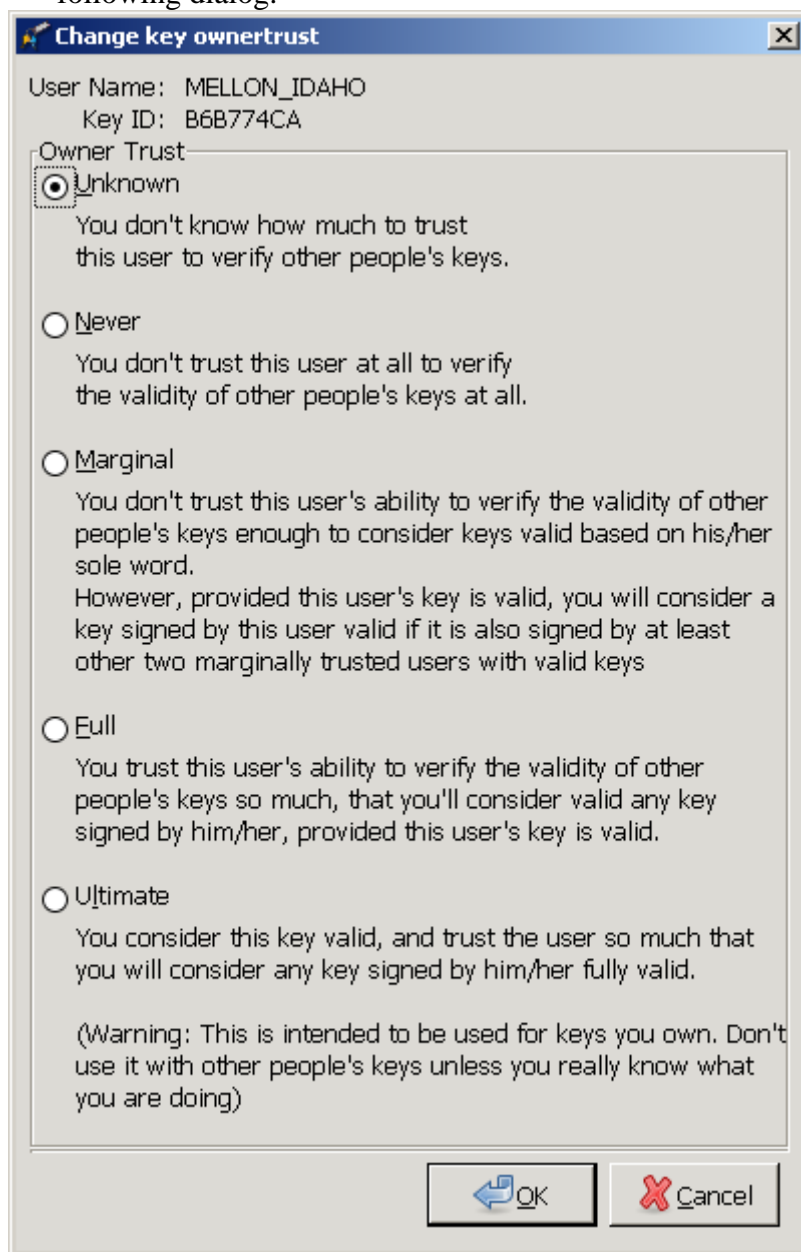


The screenshot shows the GNU Privacy Assistant - Key Manager window. The title bar reads "GNU Privacy Assistant - Key Manager". The menu bar includes "File", "Edit", "Keys", "Windows", "Server", and "Help". The toolbar contains icons for "Edit", "Delete", "Sign", "Import", "Export", "Brief", "Detailed", "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:

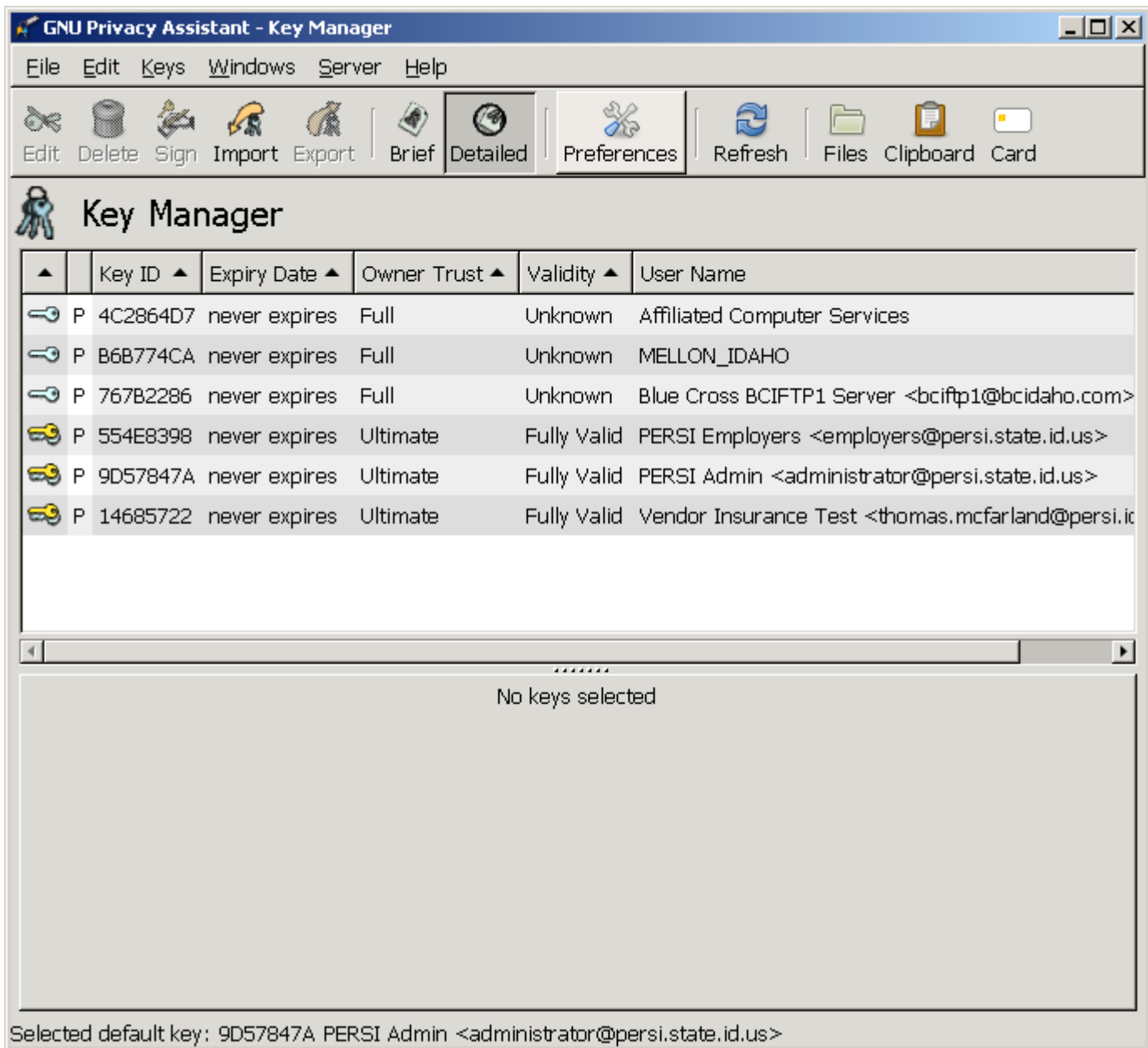
▲	Key ID ▲	Expiry Date ▲	Owner Trust ▲	Validity ▲	User Name
🔑	P 4C2864D7	never expires	Unknown	Unknown	Affiliated Computer Services
🔑	P B6B774CA	never expires	Unknown	Unknown	MELLON_IDAHO
🔑	P 767B2286	never expires	Unknown	Unknown	Blue Cross BCIFTP1 Server <bciftp1@bcidaho.com>
🔑	P 554E8398	never expires	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 individually, 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.



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



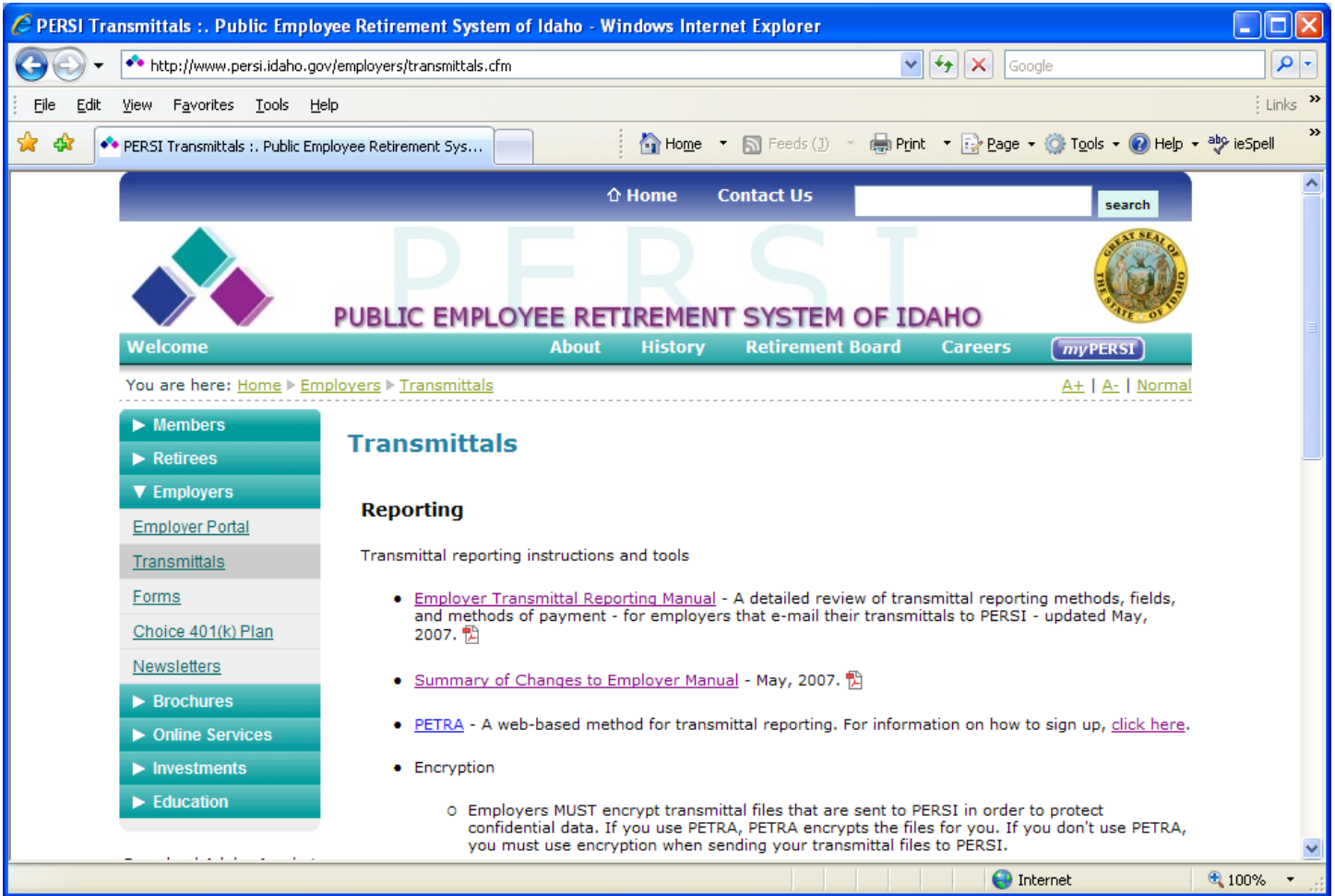
Click 'Yes'. You may have to enter your passkey to sign your partner's public key. Repeat for each public key.

*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.

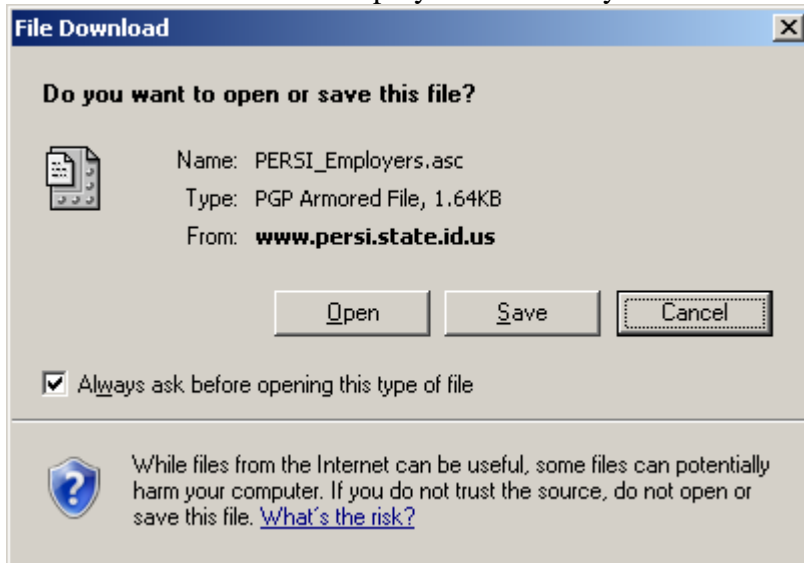
New users only!

12. Download PERSI Public key.

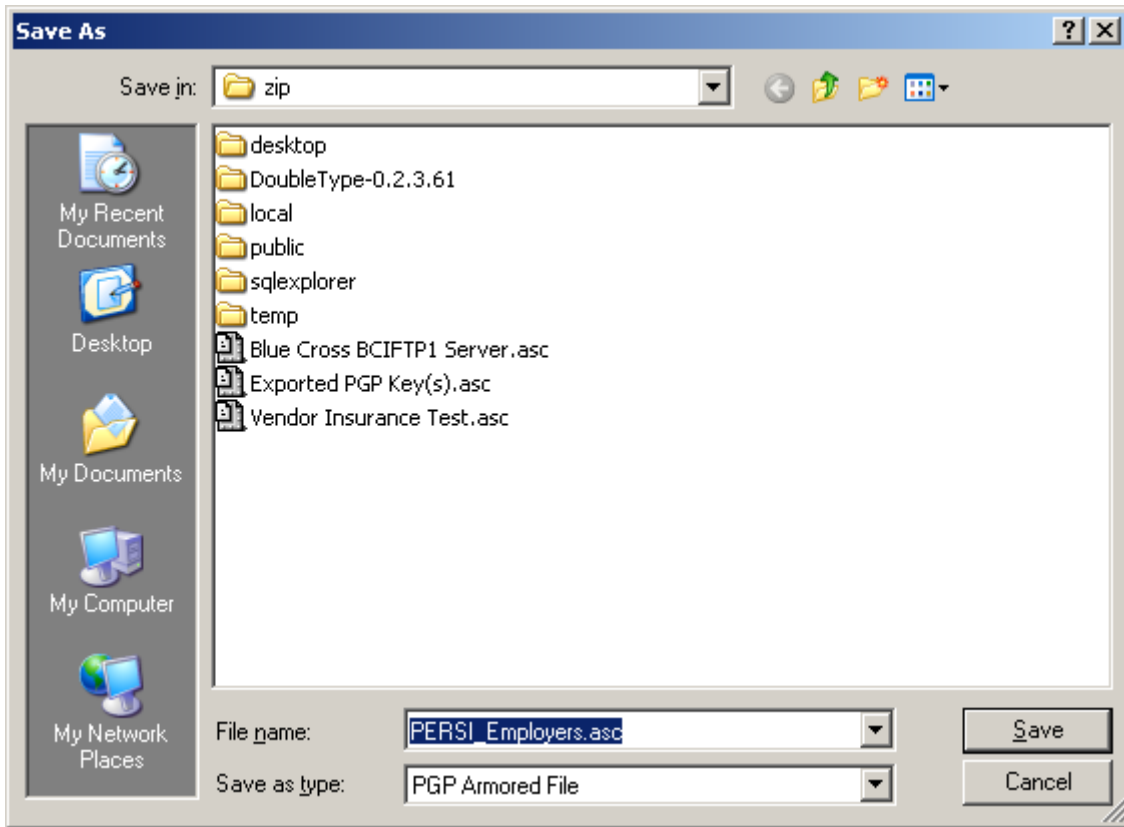
- a. Use your web browser to navigate to the PERSI employers page.
<http://www.persi.idaho.gov/employers/transmittals.cfm>



- b. Click on the “PERSI Employers Public Key” link. The download dialog will display.



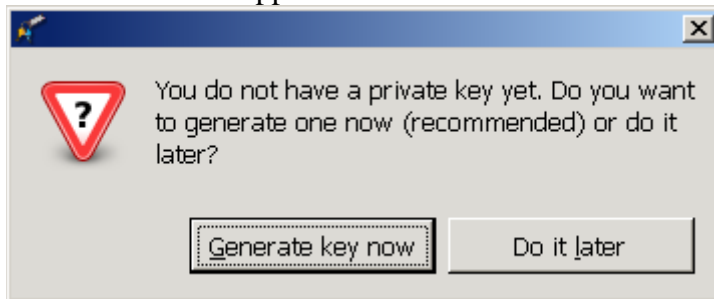
- c. Click the Save button. The save file dialog box is displayed. **(If you don't see this download dialog box, but see garbled characters, right click on the "PERSI Employers Public Key" link instead, and select "Save Target As...")**



- D. Click the Save button.

13. Create your Public/Private Key Pair.

- a. Start the GPA application.



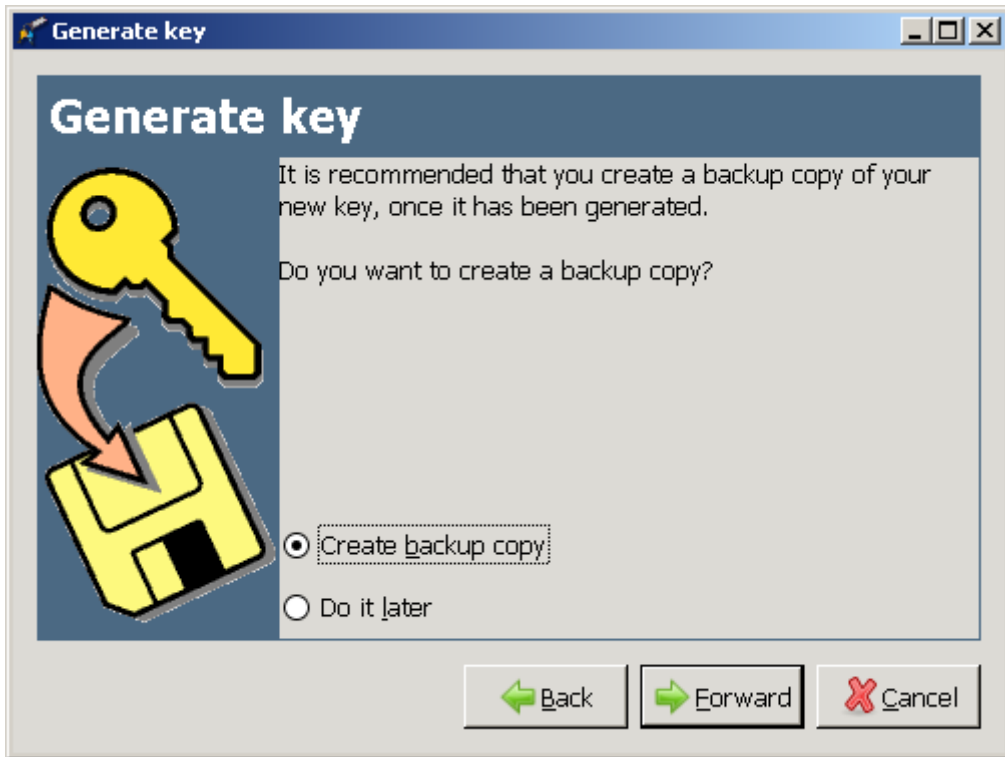
- b. Click the "Generate key now" button. The following form will display.

The screenshot shows a window titled "Generate key". On the left is an illustration of a yellow key and a person's head with a question mark and exclamation mark. The main text reads: "Please insert your full name. Your name will be part of the new key to make it easier for others to identify keys." Below this is a text input field labeled "Your Name:" containing the text "Employer Name". At the bottom right are two buttons: "Forward" with a green arrow icon and "Cancel" with a red X icon.

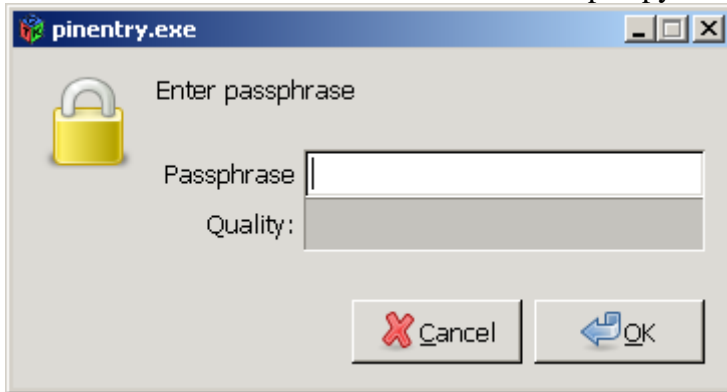
c. Enter your employer name and click the 'Forward' button.

The screenshot shows the same "Generate key" window. The main text now reads: "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." The text input field labeled "Your Email Address:" now contains the email address "thomas.mcfarland@persi.idaho.gov". The buttons at the bottom now include "Back" with a green arrow pointing left, "Forward" with a green arrow pointing right, and "Cancel" with a red X icon.

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

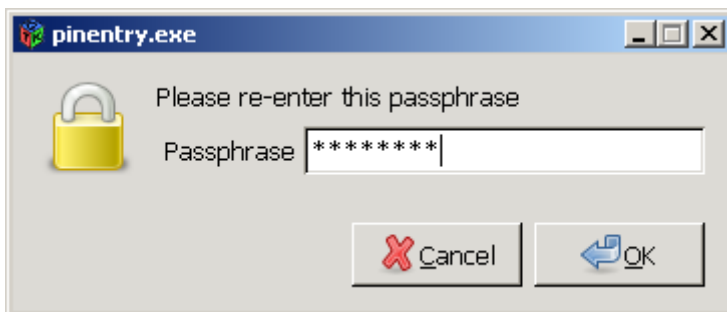


e. Leave the default selection “Create backup copy” and click the “Forward” button.

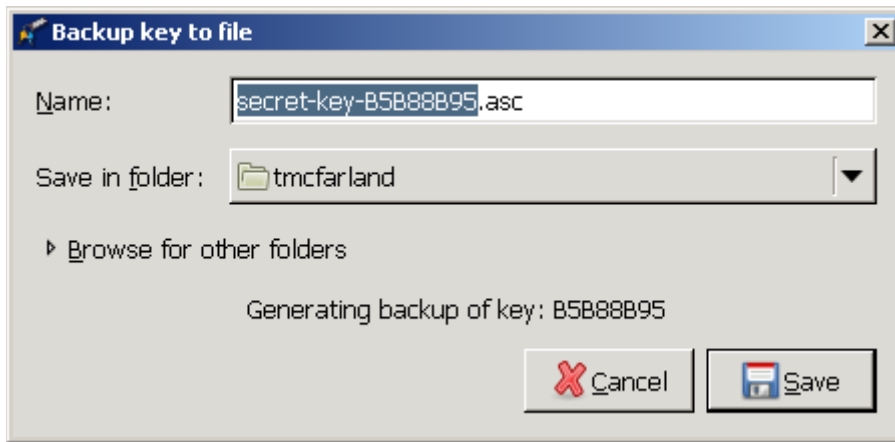


f. Enter a passphrase (you must use letters and numbers and meet minimum length requirements), then click the “OK” button.

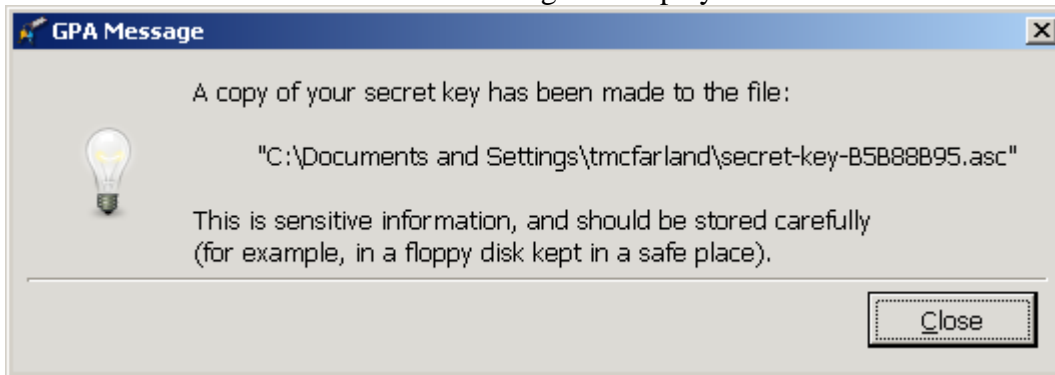
This passphrase is very important and your key pair can not be used without it. Keep it in a secure place.



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



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




i. Click the “Close” button. 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

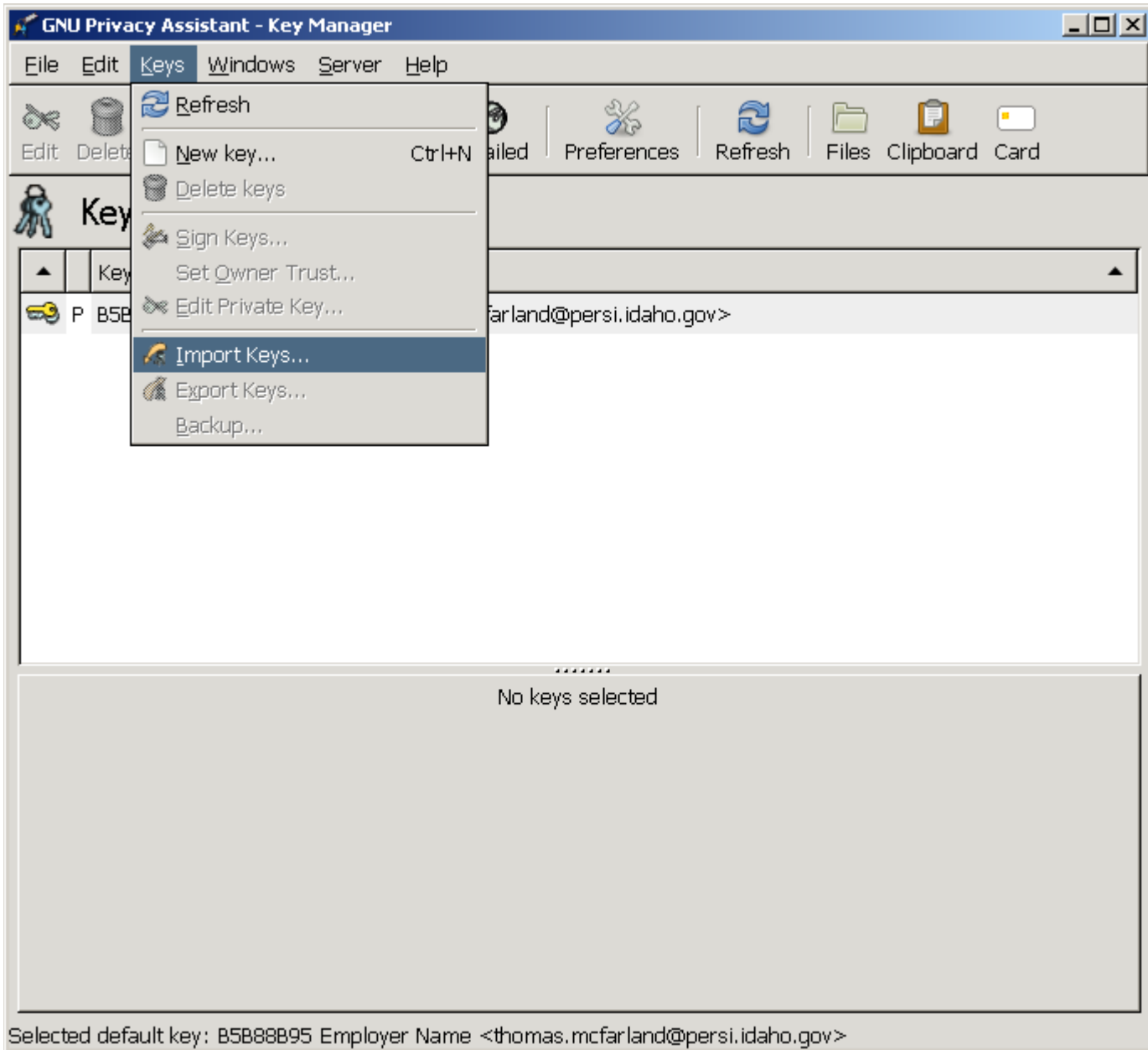
▲	Key ID ▲	User Name ▲
	P B5B88B95	Employer Name <thomas.mcfarland@persi.idaho.gov>

.....

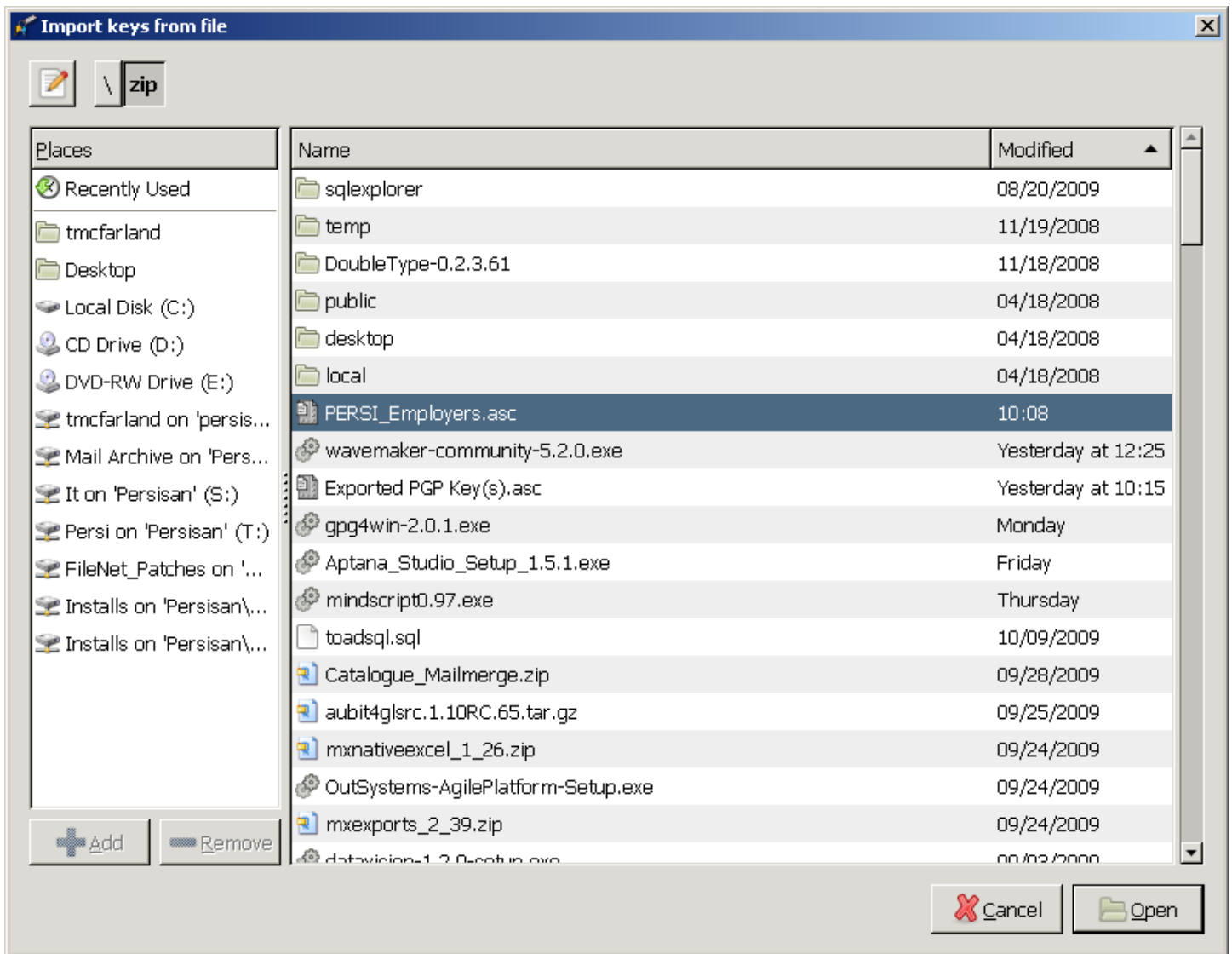
No keys selected

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

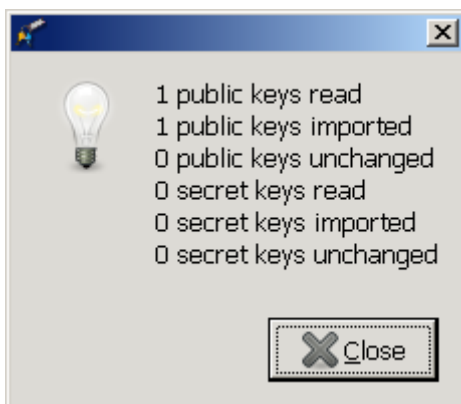
14. Import the PERSI public key into gpg4win.
 - a. Select the menu action Keys|Import .



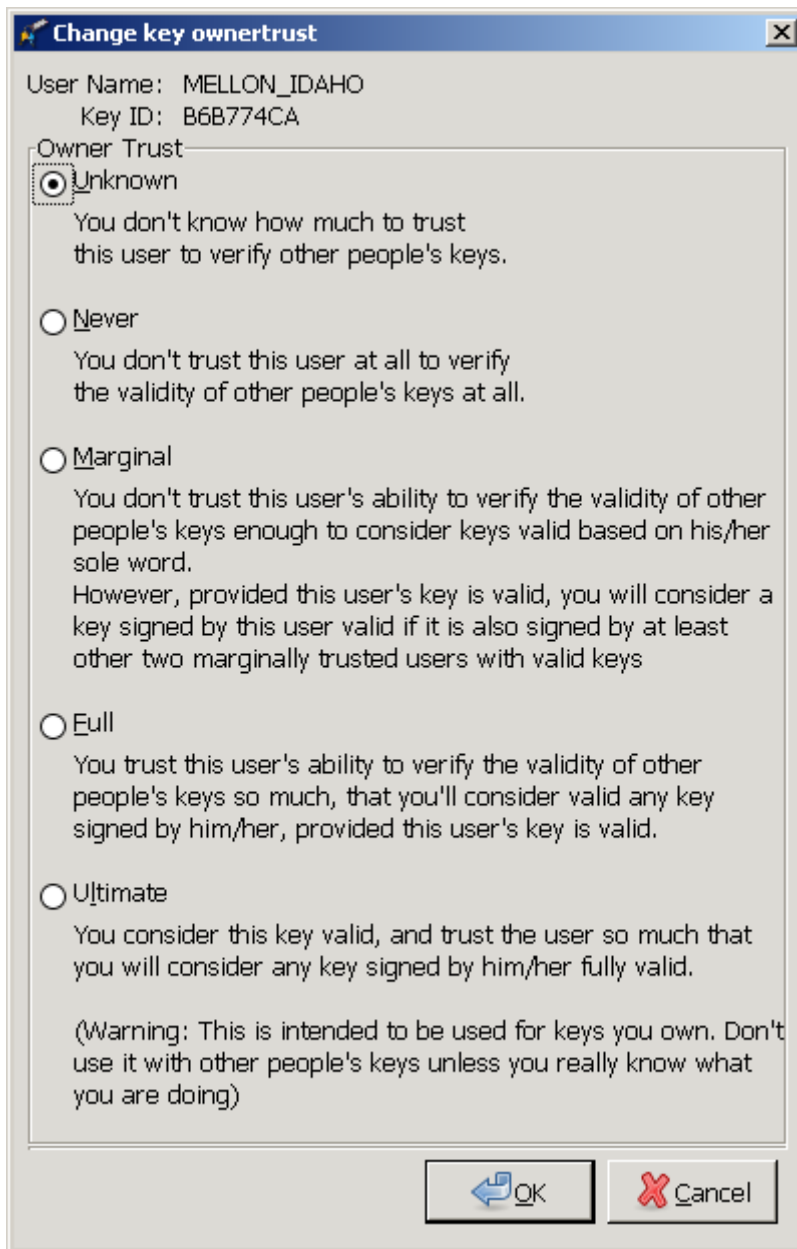
A file dialog box will be opened.



- 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 individually, then use the ‘Keys|Set Owner Trust’ menu option to display the following dialog.

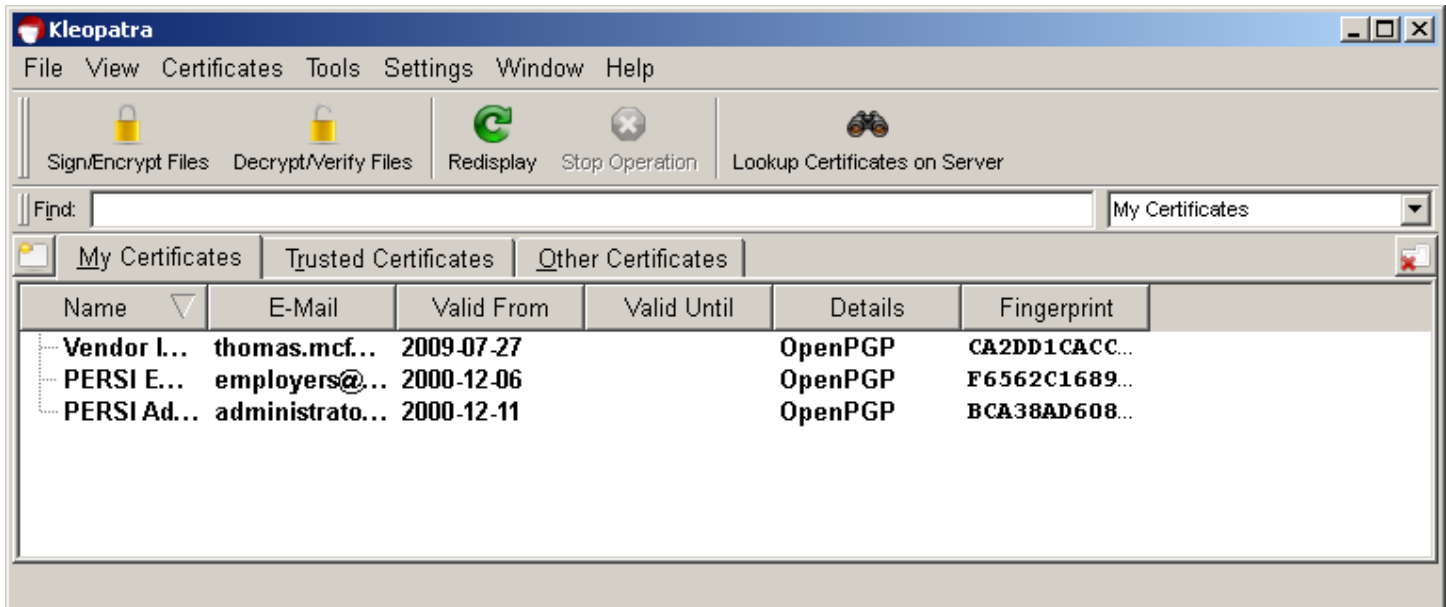


Set your own keys to 'Ultimate Trust' and other's keys to 'Full'. Click the 'OK' button. Once all of the key have their trust attribute set, close and restart the GPA application.

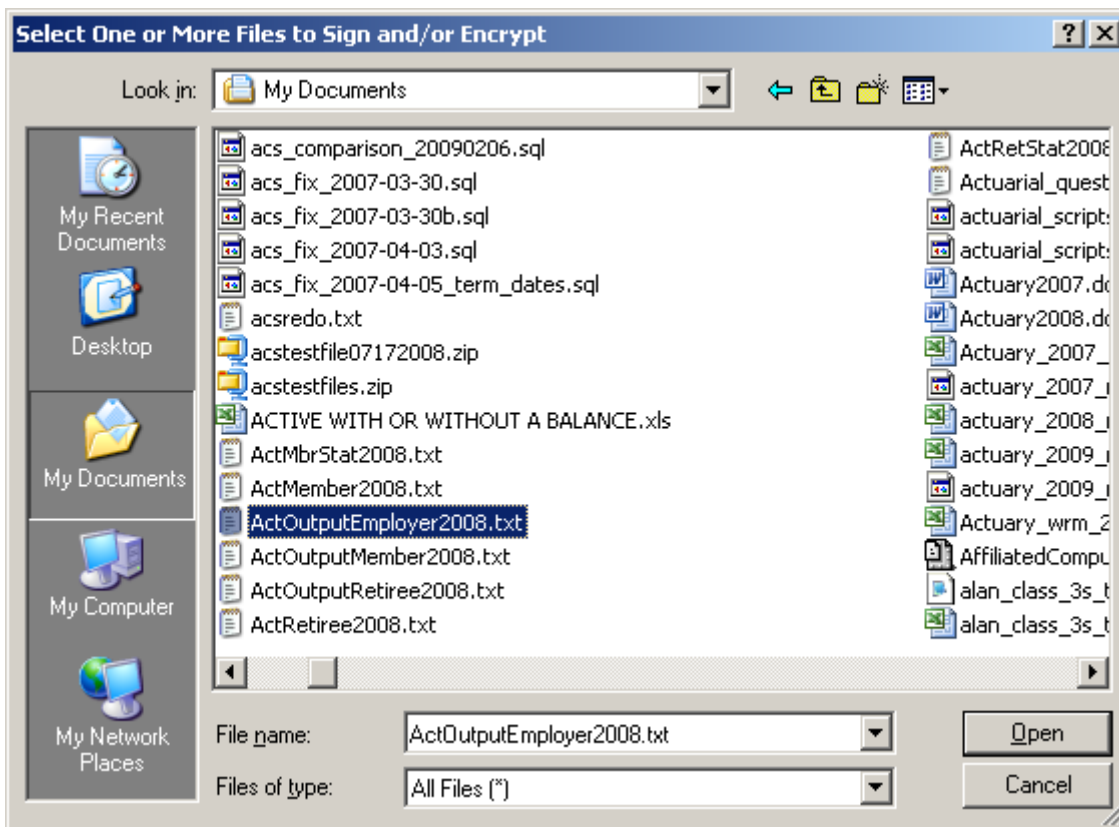
E. You are Done! Close the GPA application.

Encrypting and Signing Instructions

1. Start the Kleopatra application.

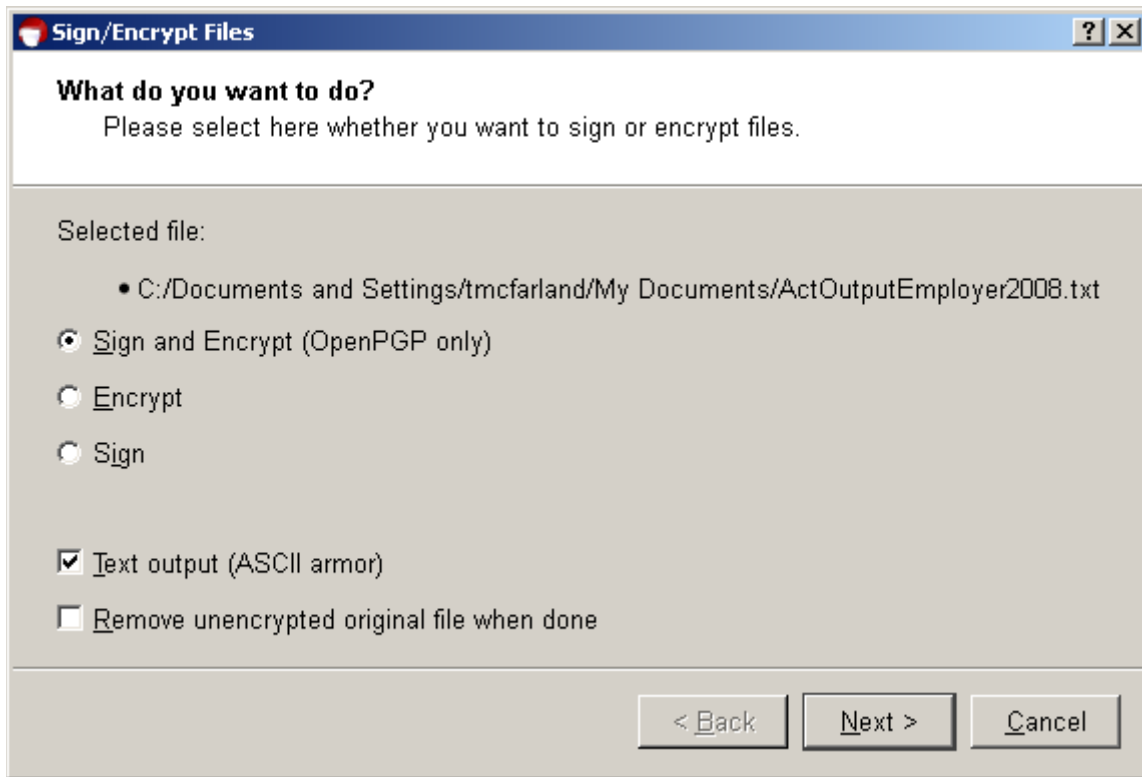


2. Click the Sign/Encrypt Files icon.



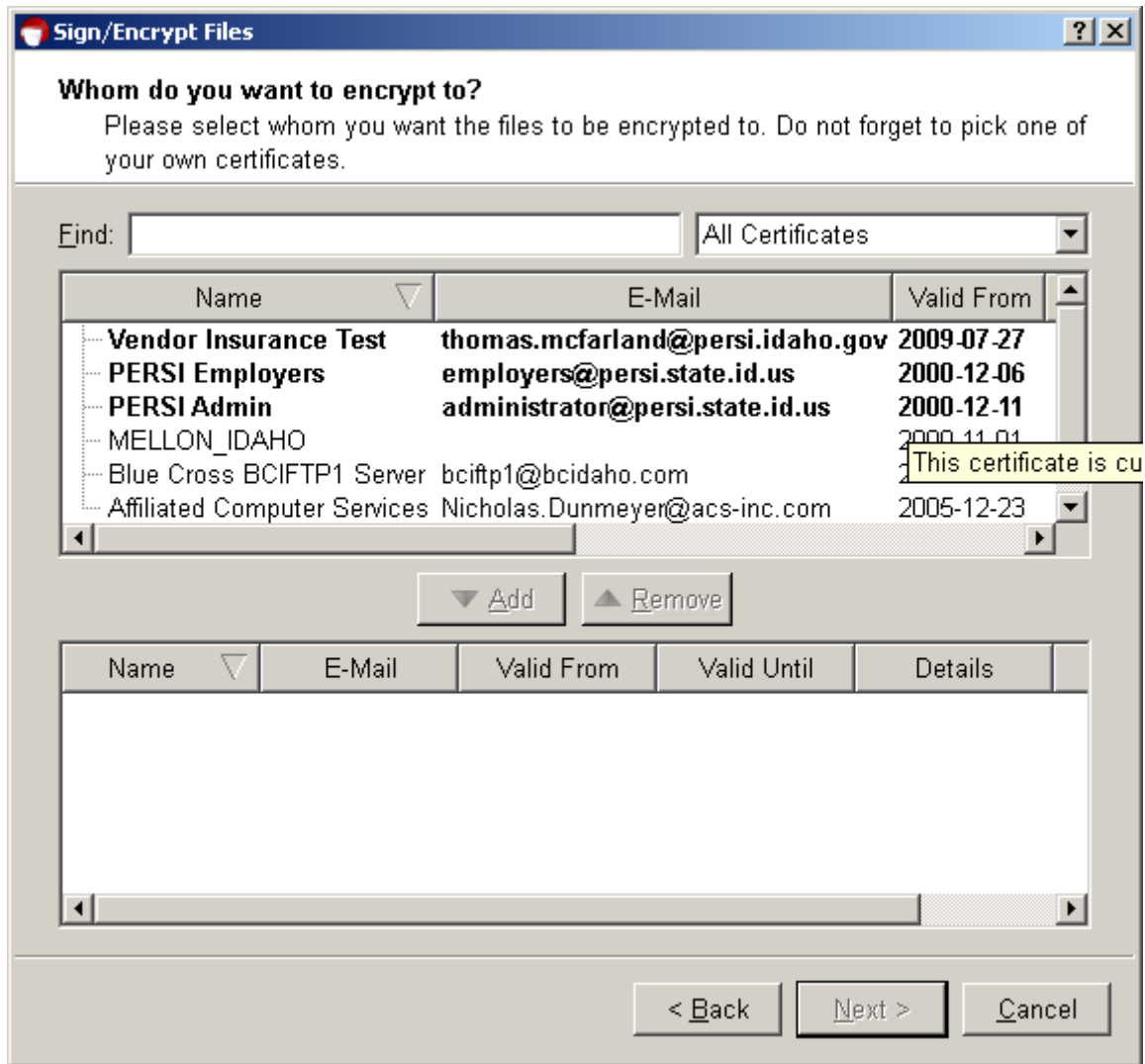
3. Navigate to find the file you want to encrypt and Click the Open button.

4. Choose your encryption options.

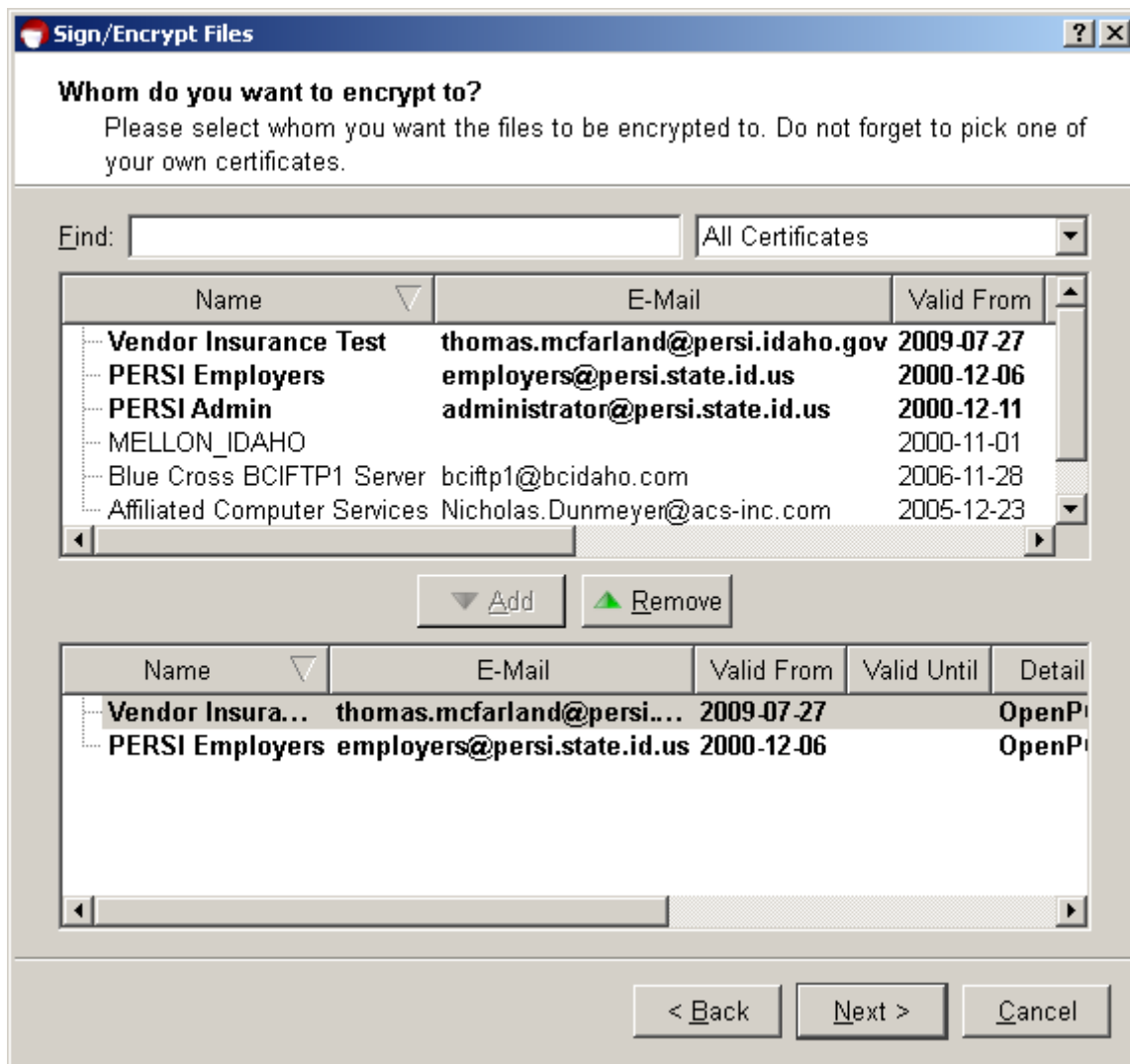


A. Click “Next”. If ‘Text output (ASCII armor)’ is unchecked the file will encrypt but have a .gpg extension.

5. Select the recipients for the file.

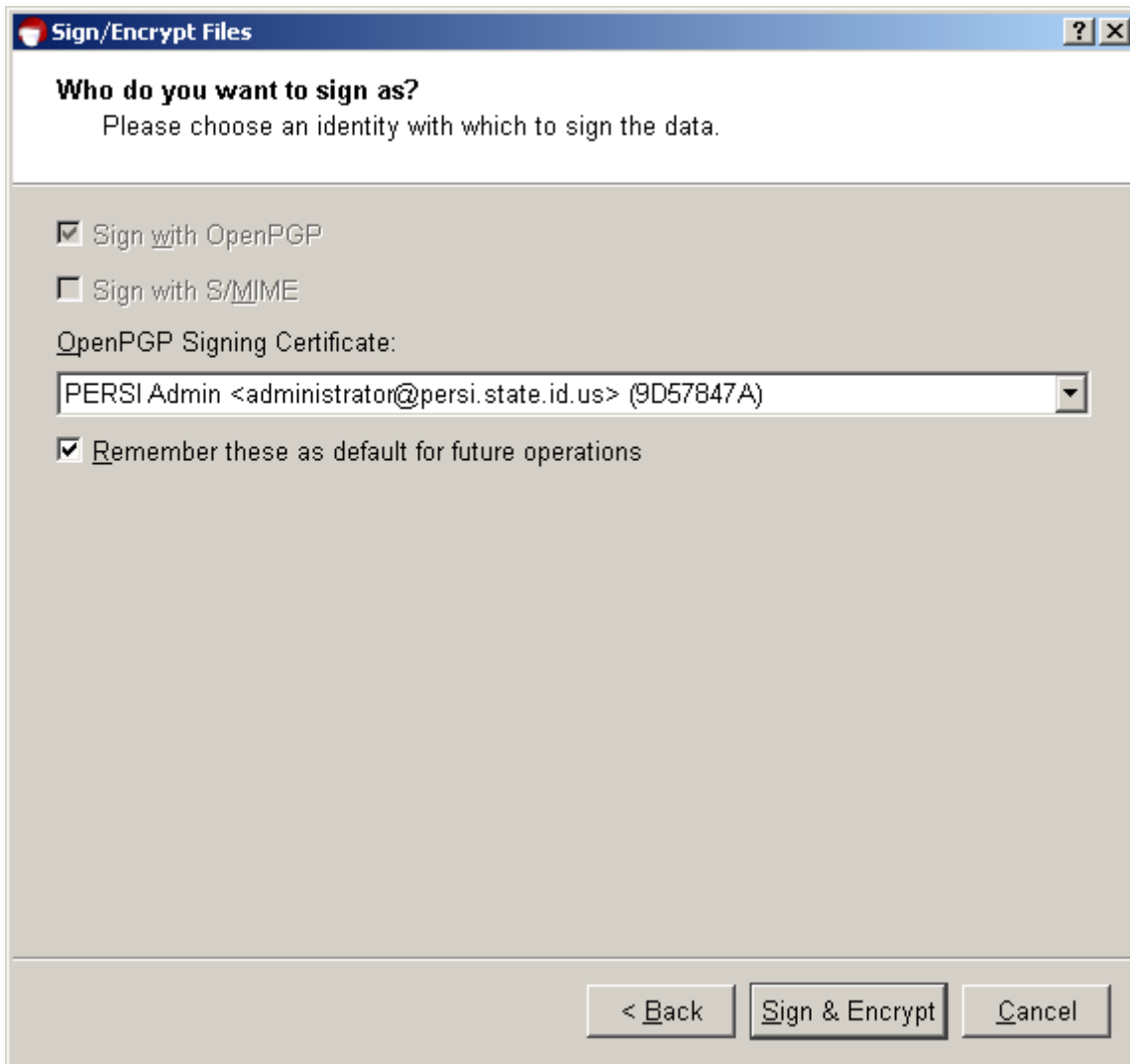


6. Highlight the recipient name(s) and click the add button.



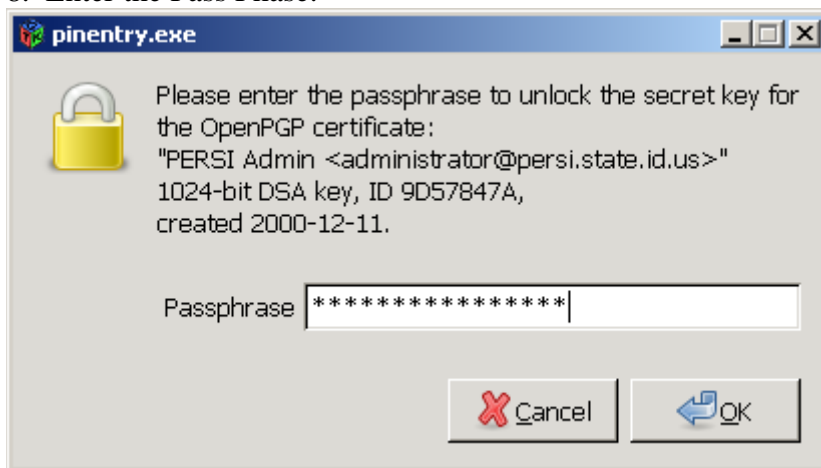
A. Click the "Next" button.

7. Choose the signing key.



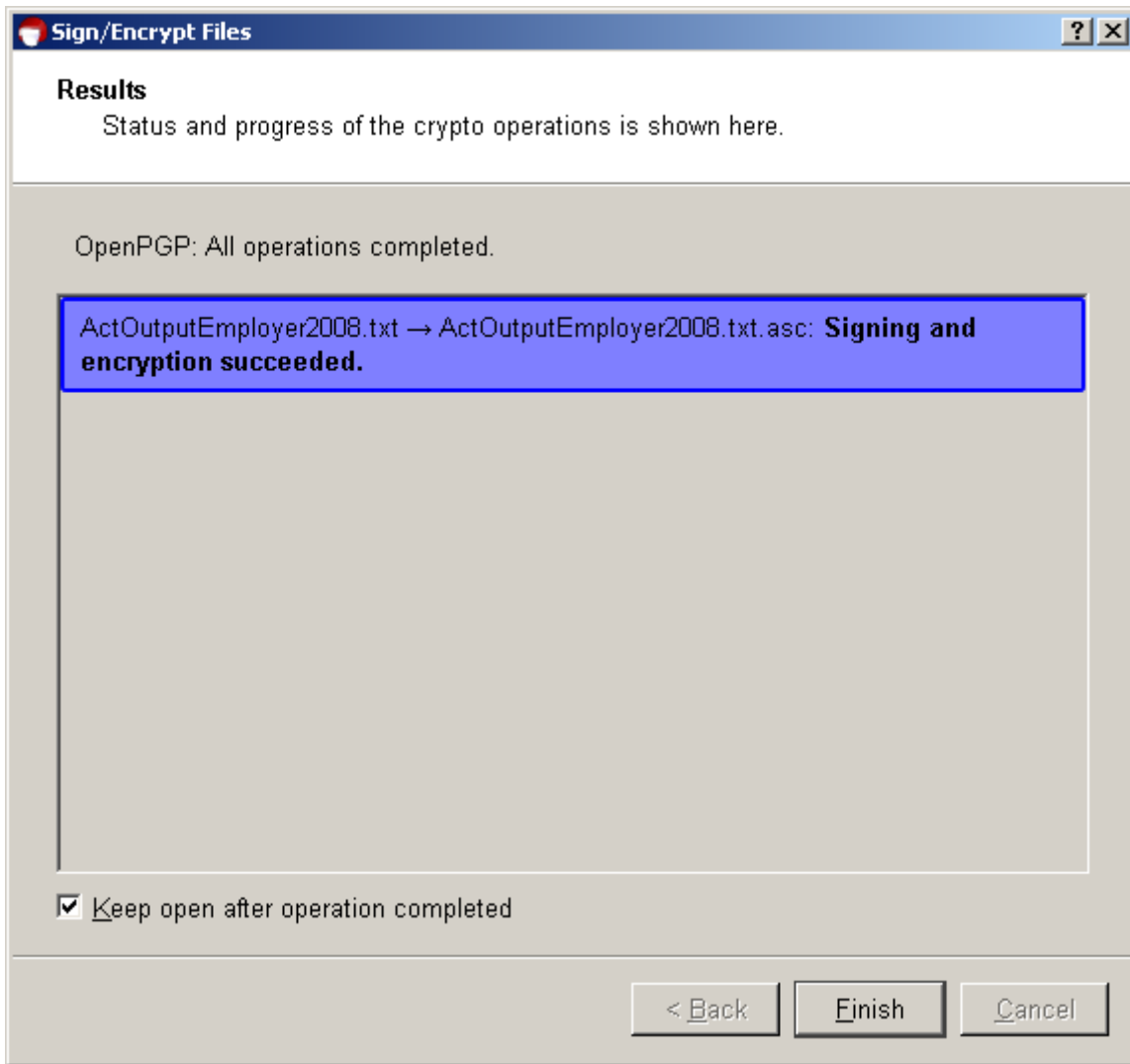
A. Click the Sign & Encrypt button.

8. Enter the Pass Phase.



A. Click "Ok".

9. View the results screen.

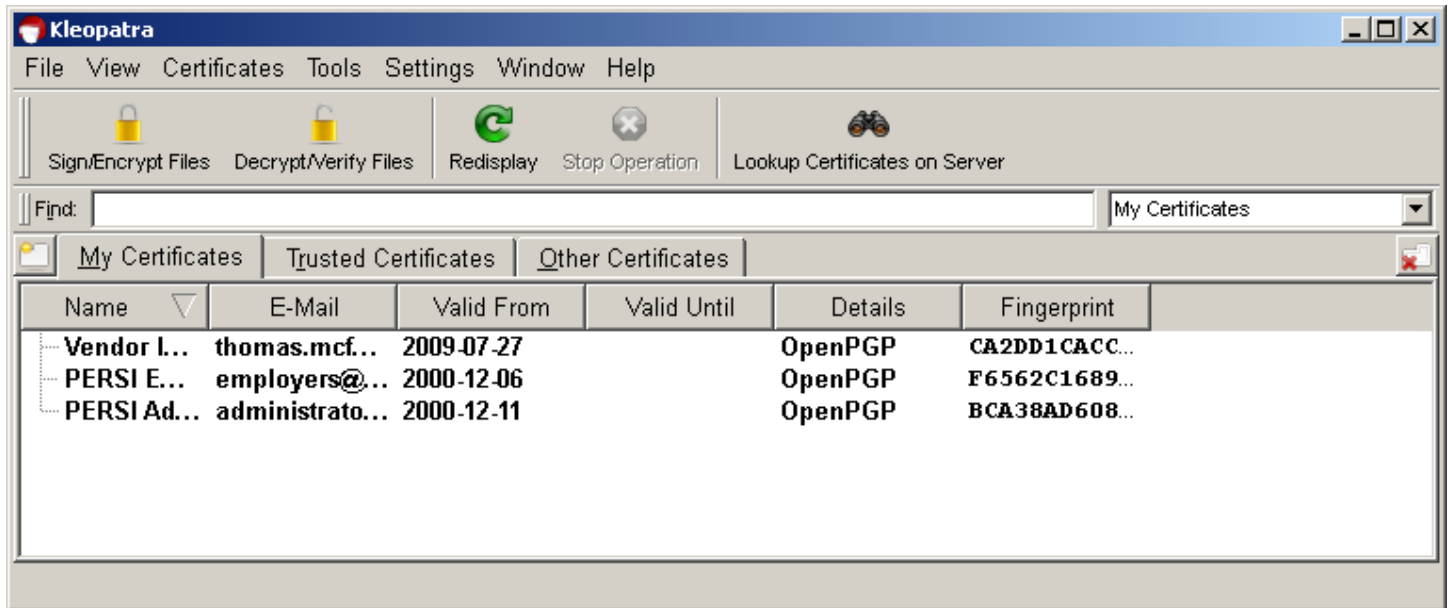


A. Click "Finish".

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.

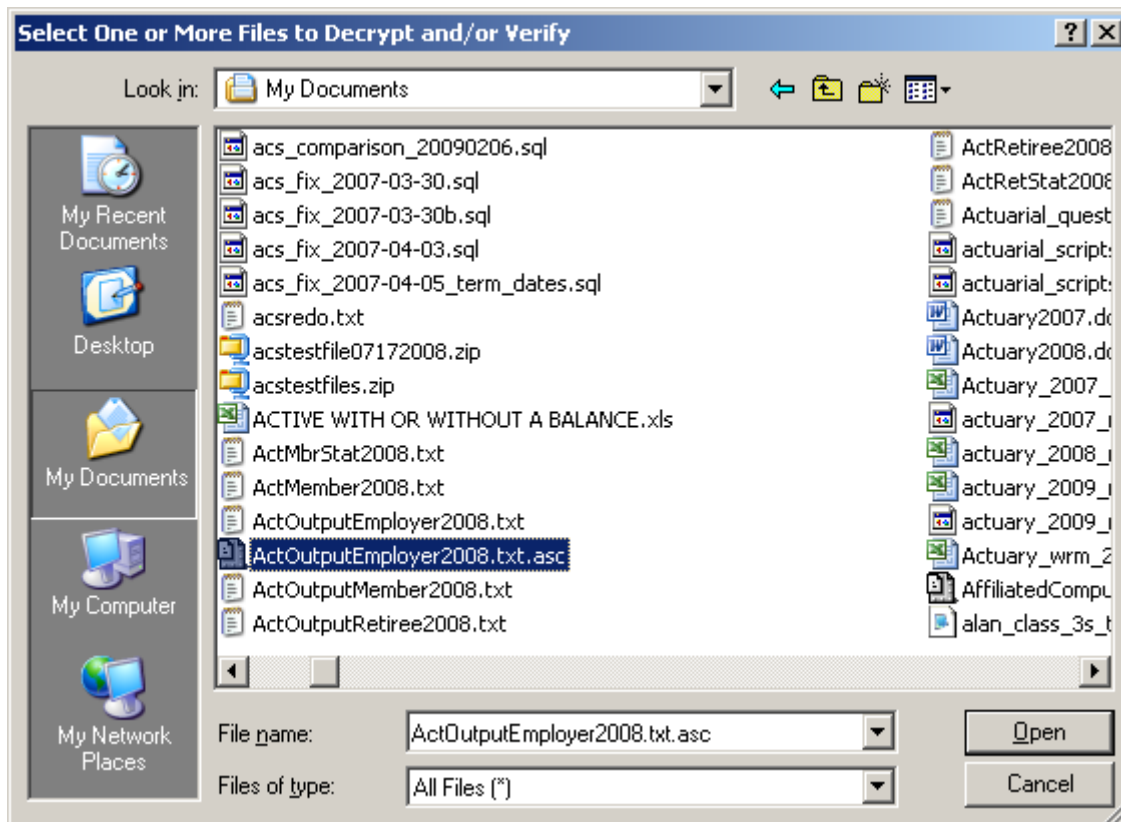
Decrypting Instructions

1. Start the Kleopatra application.



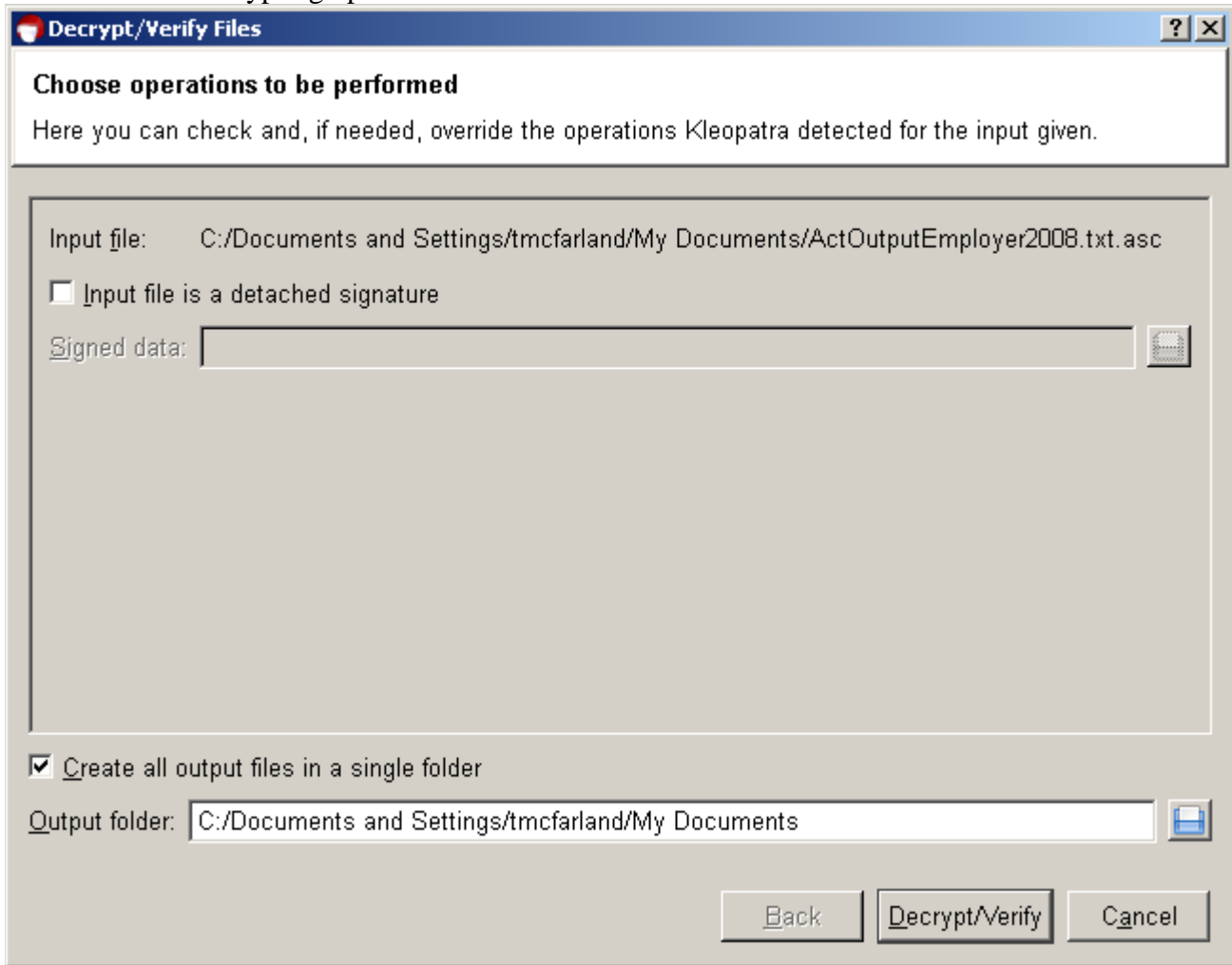
A. Click the Decrypt/Verify Files icon.

2. Navigate and select the file to decrypt.



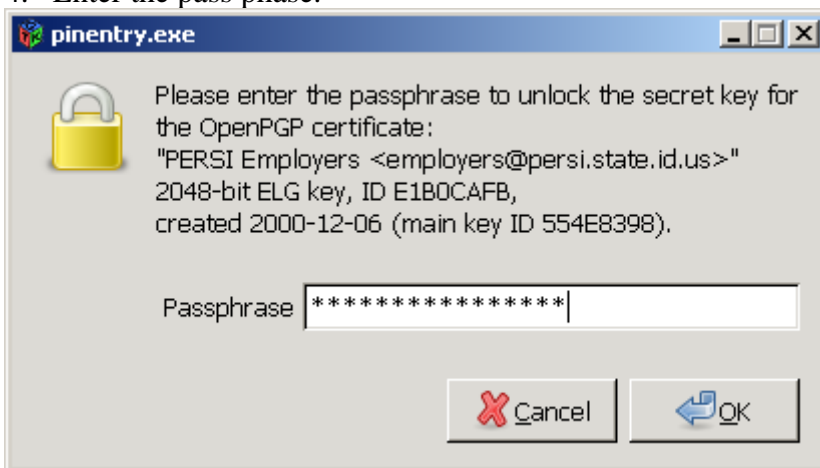
A. Click the Open button.

3. Choose the decrypting options.



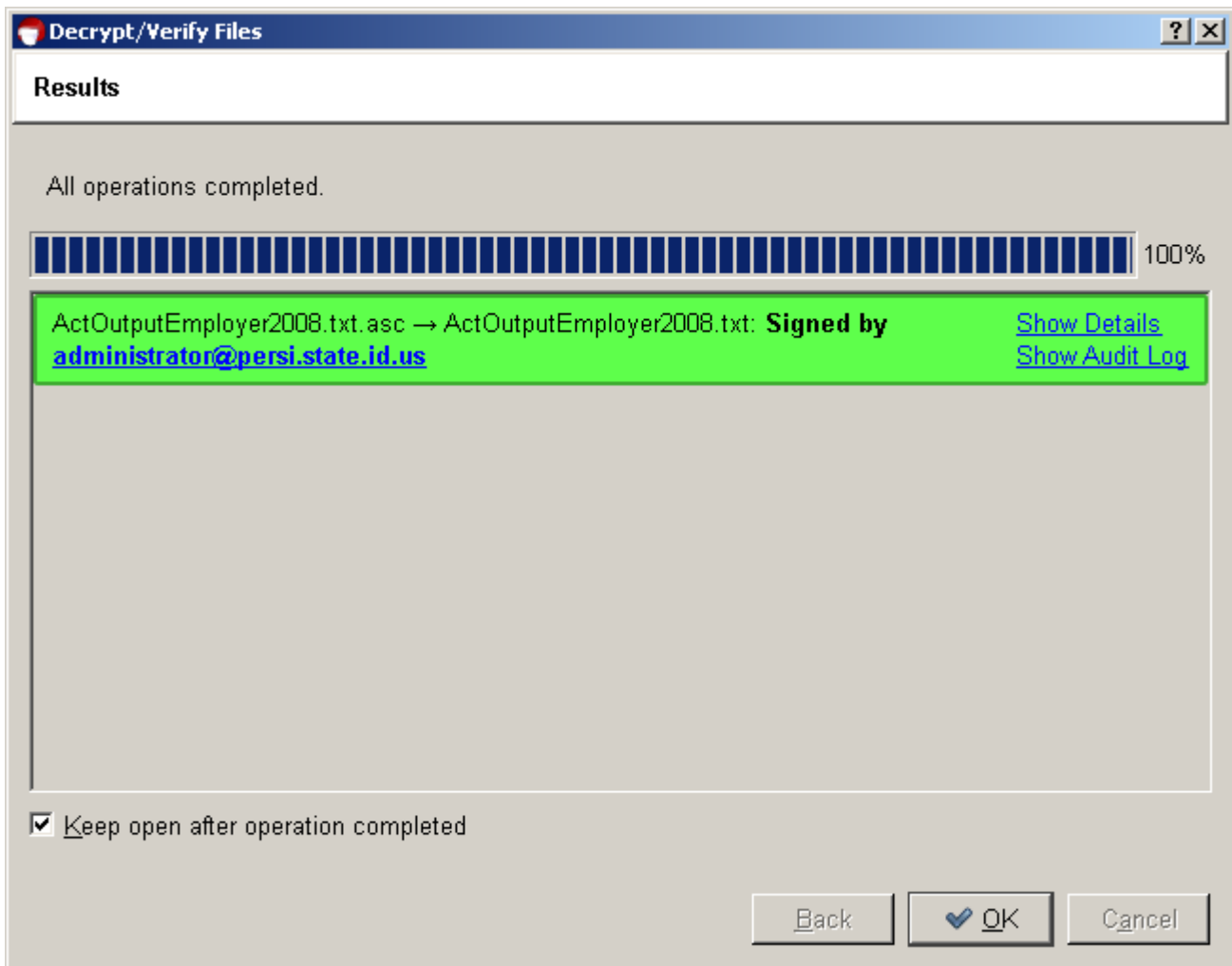
A. Click the Decrypt/Verify button.

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