EUROPEAN COMMISSION
EUROSTAT

Directorate B: Statistical Methods and Tools; Dissemination
Unit B2: LSA

File Ciphering for Secure Data Exchange

Installation / User guide for external Partner

Date 21.10.2008
Author Peter Weiss
Eurostat / B2

Table of Contents

1. Introduction

Today it is very important to protect data which are sent to others over insecure communication channels, in particular with regard to the increasing number of people who are trying with malice aforethought to get access to this data.

In order to prevent the unauthorised access to statistical data it is necessary to increase the protection level for file transmission between Eurostat and the partner in the member states.

This aim can be achieved by using a cryptographic application. Based on the open source encryption software **WinPT / GnuPG**, which was selected to protect the data, the idea is to encrypt the file with the statistical data and send it via **eDAMIS** to the recipient. The receiver will then decipher the coded file with the same software.

The main advantages of the selected application are among other things:

- the software package is free for commercial and personal use
- the installation of WinPT / GnuPG on Windows systems is easy
- the handling is user friendly
- there is no password which has to be exchanged

The following document contains a short description about the used cryptographic method. Furthermore you will find instructions about the installation of the encryption software and how to extract the public key. Finally there is a description what to do in order to decipher coded files you have received from Eurostat.

2. Background Information

If you have to send information to someone else and you want to keep it a secret, hide it in another message so that only the right recipient will understand.
Many creative methods of hiding messages have been invented over the ages. Cryptography in the computer age typically involves the translation of the original message into a new and incomprehensible one by a mathematical algorithm using a specific 'key'. Just like you need to open the lock on a door with a key, the algorithm and key protect the contents of your message from unauthorized access.

There are three primary cryptographic techniques. Two are used to encrypt information in a form that can be recovered only by someone who has an appropriate key. The third, which will not be explained in this document, used in authentication and integrity schemes, scrambles input without any intention to recover it.

2.1 Conventional Cryptography

The conventional cryptography uses a single key to encrypt and decrypt a message. An algorithm that uses only one key for coding and decoding is called ***symmetric***.

Two parties who are using a symmetric cipher must agree on the key beforehand. Once they agree, the sender encrypts a plaintext using the key, sends it to the receiver, and the receiver decrypts the ciphertext using the same key. An example is the well known application WinZip.

However concerning the security of this procedure, the main problem is not the security of the symmetric key but with the key exchange. For an attacker it is probably much easier to intercept the key when it will be exchanged compared to the cost to guess the right key.

2.2 Public Key Cryptography

In order to eliminate the problem of insecure exchanging keys in advance, the public key method can be used. Two keys, which are mathematically uniquely linked together, are used in this scheme, one to encrypt and one to decrypt. Thus this algorithm is called ***asymmetric*.** The underlying idea is that every person which is using this method has a pair of keys in which one key is held private while the other one is made publicly available. To send a message to someone, you encrypt it with the recipient's public key. The recipient then decrypts it with his or her private key.

Concerning the transmission of statistical data this means, shortly after Eurostat has received your public key, you can decipher coded files of Eurostat with the appropriate private key on your PC.

2.3 WinPT/GnuPG

The application which has been selected to use the public key cryptography method is the open source software package WinPT / GnuPG. Both are free programs under the GNU General Public License.

GnuPG
GnuPG is Gnu Privacy Guard and is the actual engine that does the encryption. It is a command line program when used alone.

WinPT
WinPT (Windows Privacy Tool) is the graphical front end to GnuPG that runs on Windows operation systems. It is easy to install and to use.
The application is divided into several, so-called managers. There is a manager for the key (ring), for files and for smart cards.

3. WinPT Installation / Key Generation

General

You have received the following two files from your partner in Eurostat.

-	gnupt-2.7.2_gpg1.4.2-wpt0.10.1-gpgrelay0.959-int.exe	Installation procedure for WinPT / GnuPG. The package contains the following software versions GnuPG 1.4.2 WinPT 0.10.1
-	WinPT_documentation.xxx	Description how to install, configure and to use WinPT (this document).

Requirements

Copy the executable file to any convenient directory on your PC. Take note of this location as it will be required later on.

WinPT application is a PC based software which requires a minimum environment to run under a Windows operation system:

- Windows 98/2000/XP operation system. However the program also works on NT/95/ME but Windows XP or better is recommended.
- 128 MB RAM (at least).
- 3.5 MB disk space for initial installer storage.

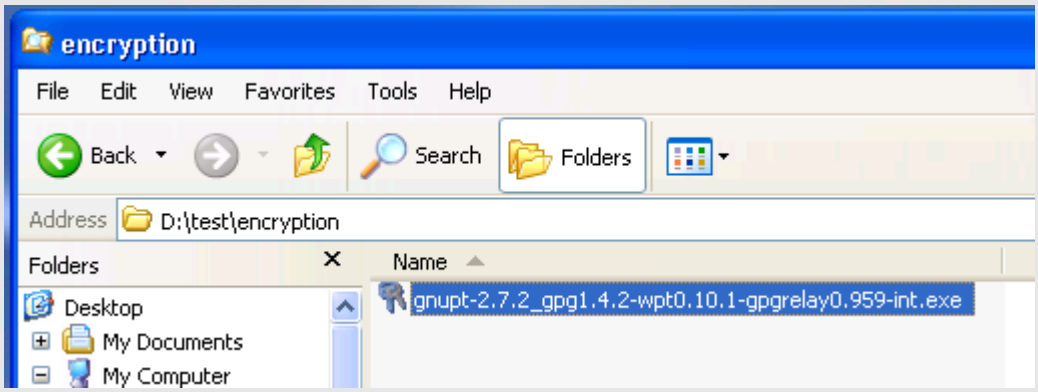
It is <u>not</u> necessary to have administrator rights on the PC for installing the application.

3.1 WinPT Installation

Start Installation

- Stop all other programs running on your PC.
- Open the directory where you have stored the two files received from Eurostat (see page 6).
- Start the installation by double-clicking the file

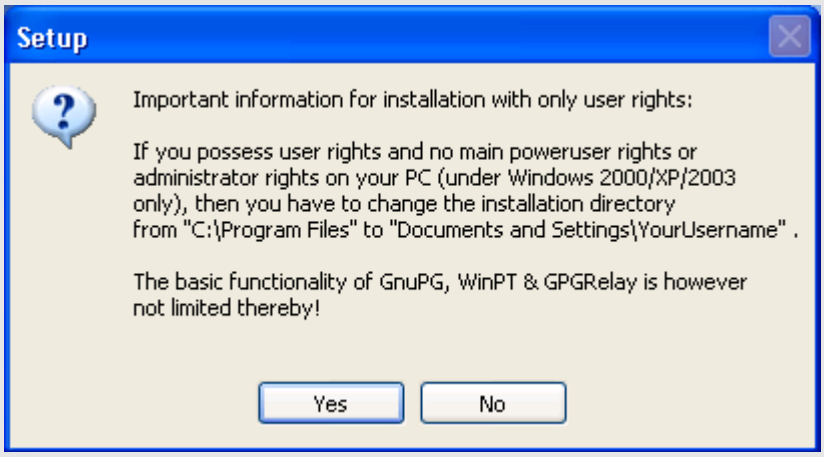
  gnupt-2.7.2_gpg1.4.2-wpt0.10.1-gpgrelay0.959-int.exe.



Necessary permission

- A small pop-up window appears. It contains information about the required installation directory, depending on the rights your account has. You will need this information at a later date.
  In case your account possess administrator rights you can choose any convenient directory otherwise select as directory "C:\Documents and Settings\YourUsername".

- Click **Yes.**



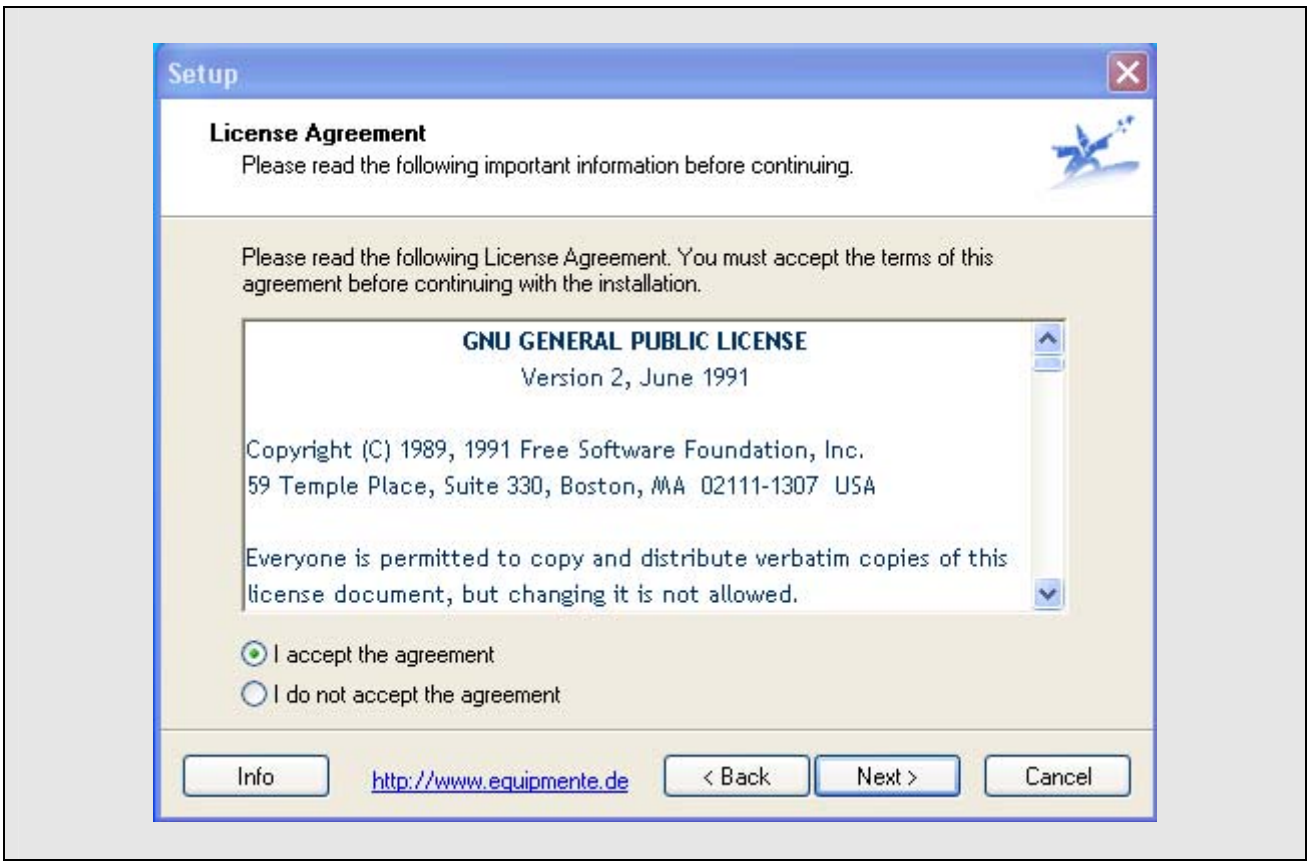
Wizard Installer

- Reminder: there should be no other applications running on your PC.

- Click **Next.**

License Agreement

- Select the '**I accept the agreement**' button in order to confirm the License Agreement.
- Click **Next**



Installation Information

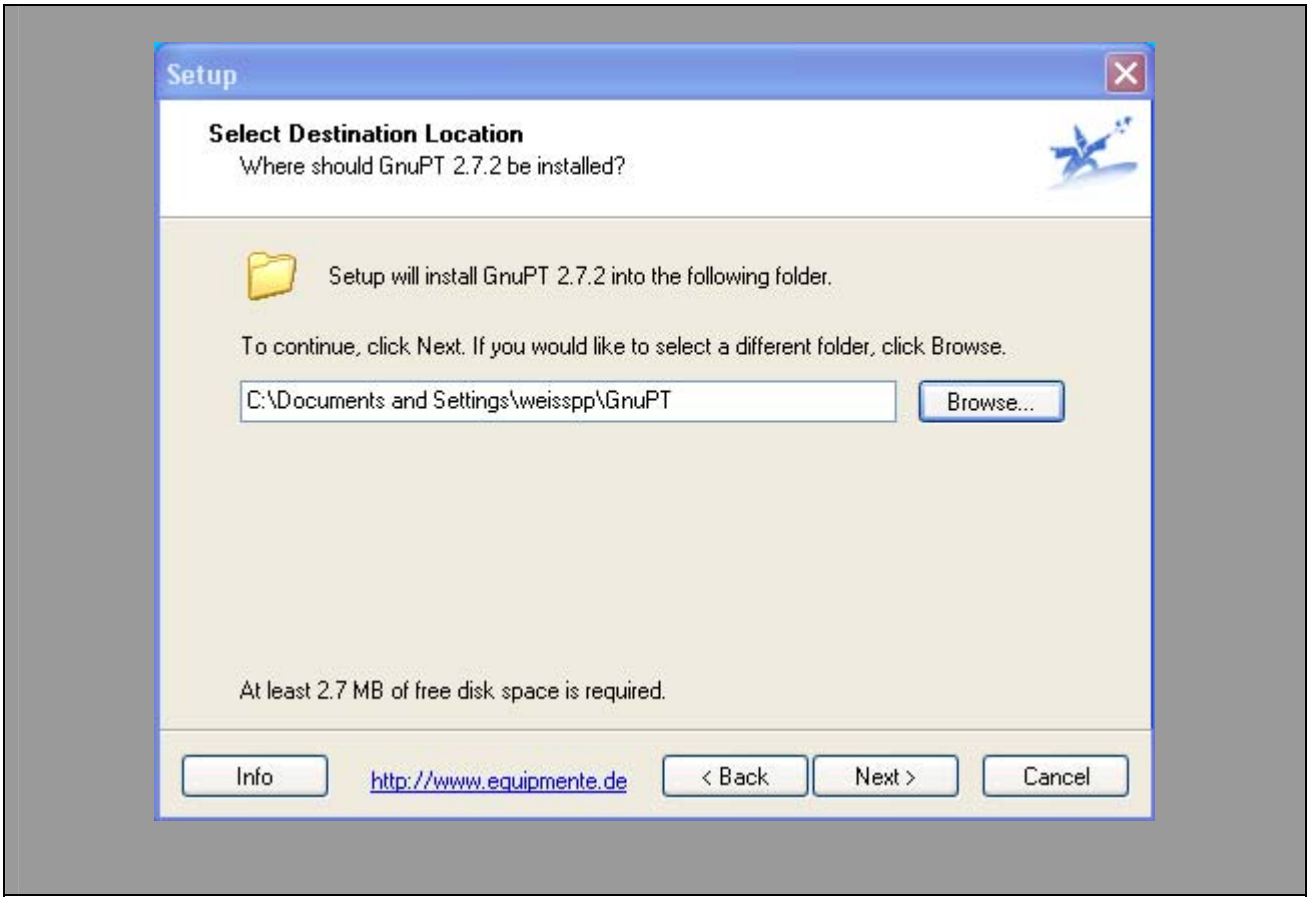
The next window is informing you about the possible components which will be installed by default.

- Click **Next**

Choose Installation Location

- Confirm the destination folder or enter your own. The default folder is *C*:\Program Files\GnuPT.
  In case your account doesn't has administrative rights choose as installation directory C:\Documents and Settings\YourAccount (see also page 8 - Necessary permission -)

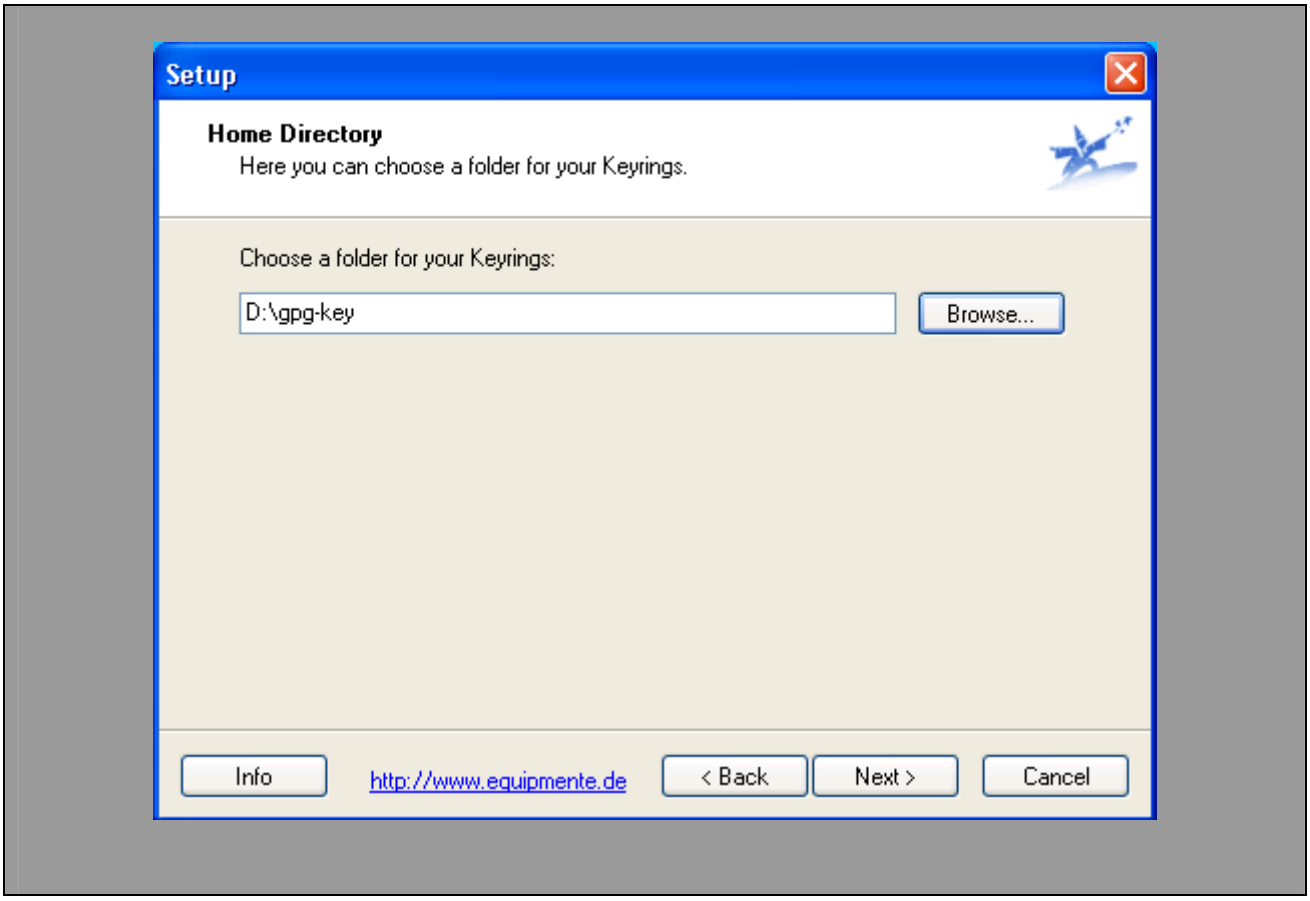
- Click **Next** to continue.



Choose Keyring Location

Select a directory where you want to store the keypair, i.e. both the public and the private key. You can select any convenient directory you want.

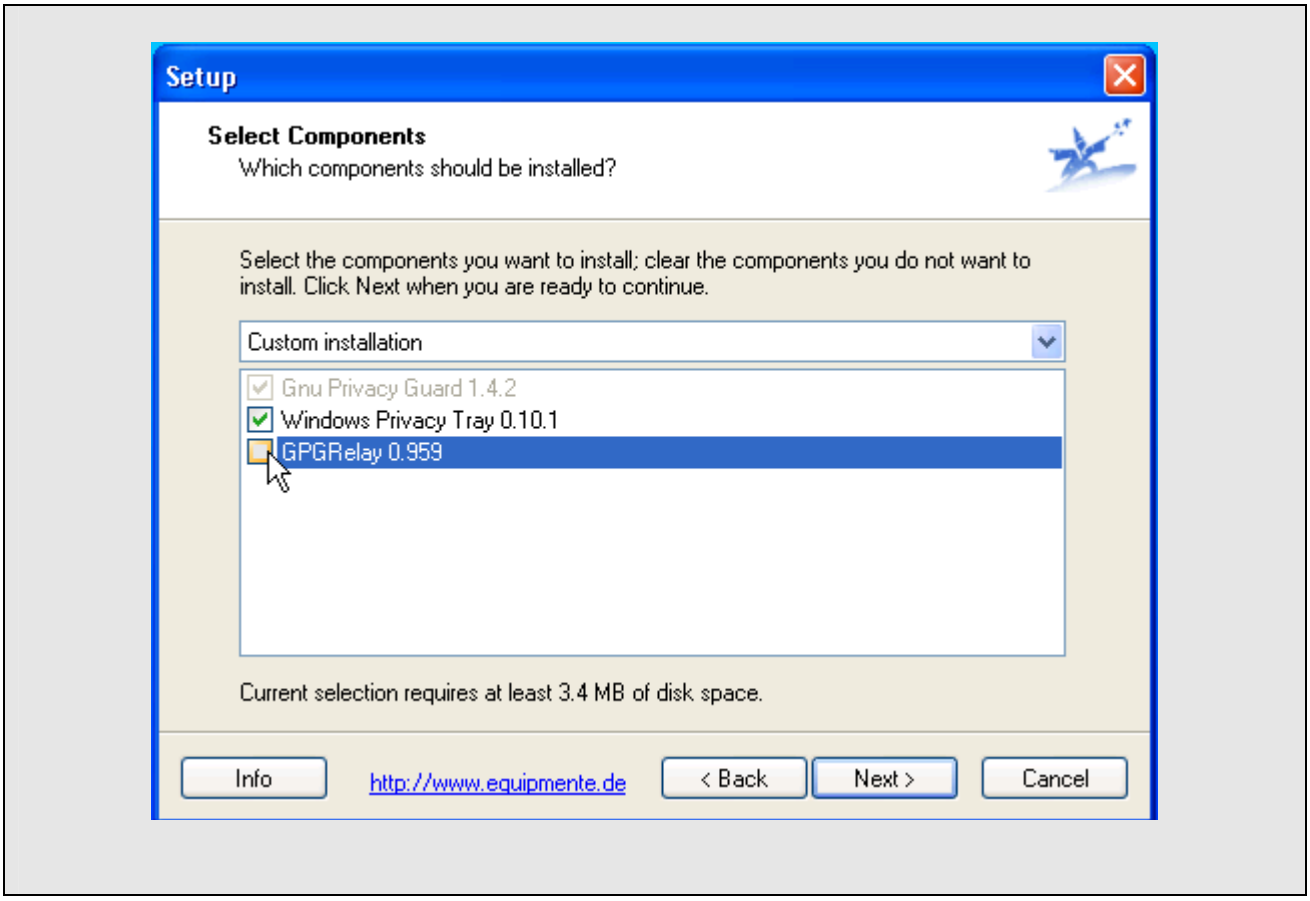
- Click **Next** to continue.



Choose Components

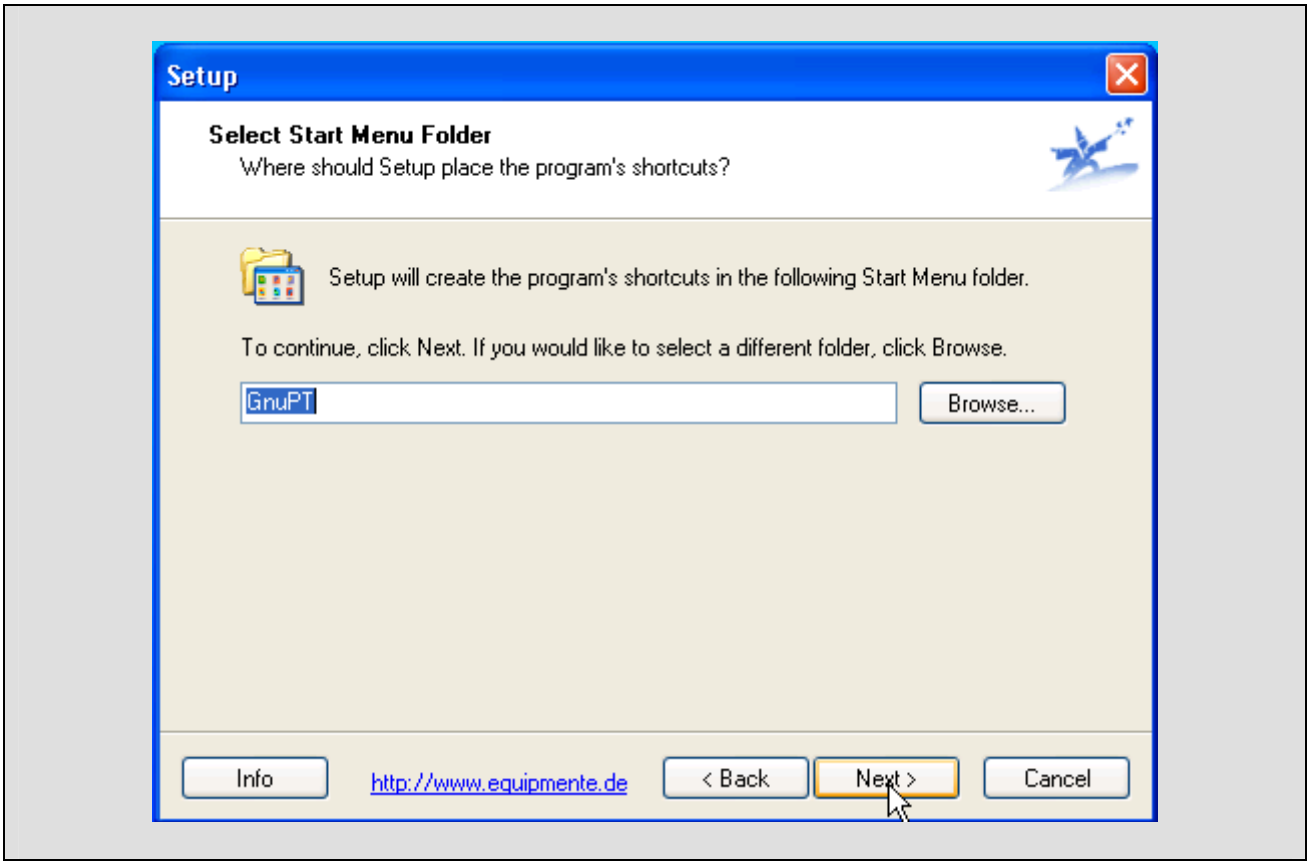
- Deselect in the following window the component GPGRelay. This application will not be used.

- Click **Next** to continue.



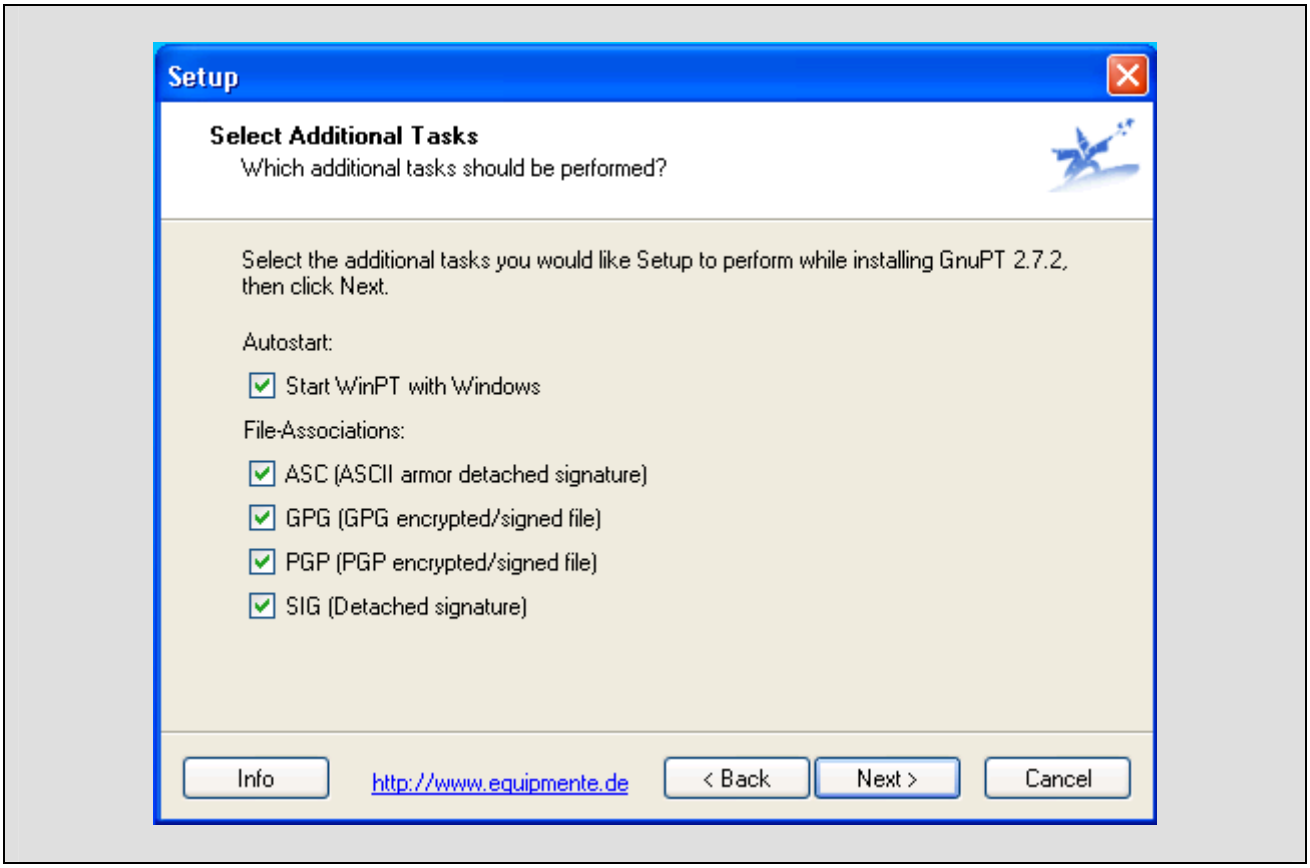
Choose Start Menu Folder

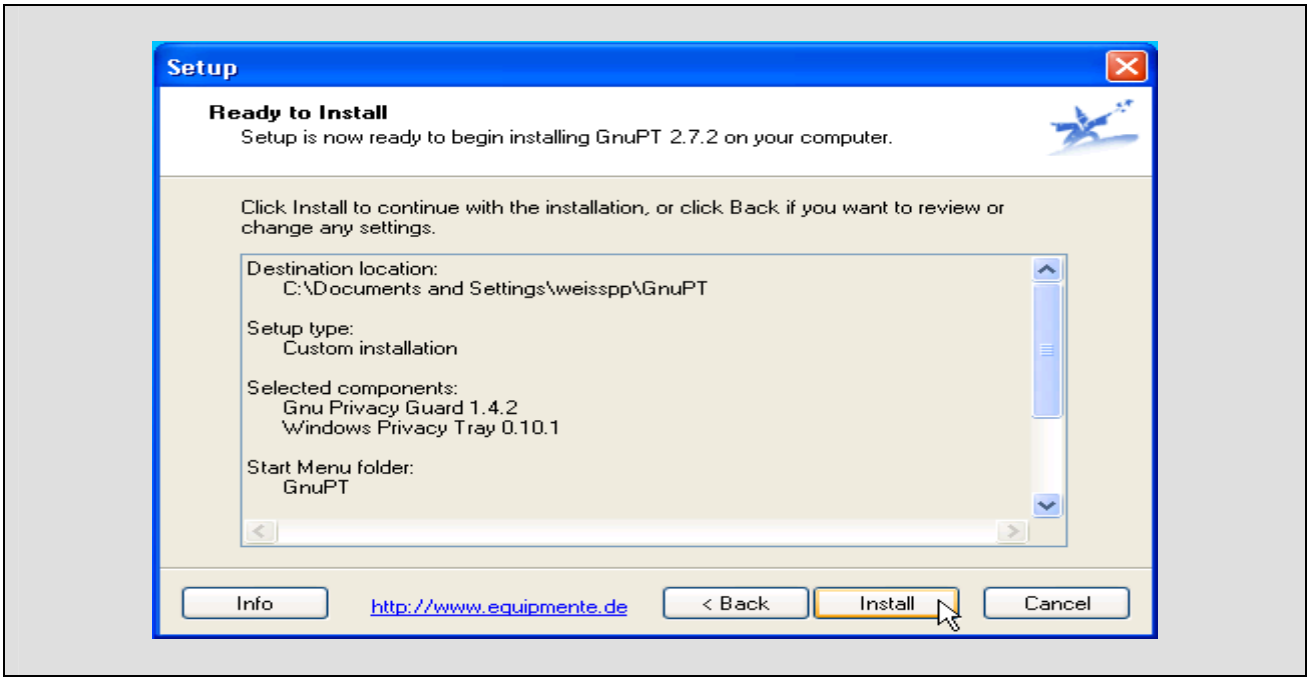
- Confirm the default Start Menu folder (Windows Privacy Tools), or enter your own.
- Click **Next** to continue.



Select Additional Tasks

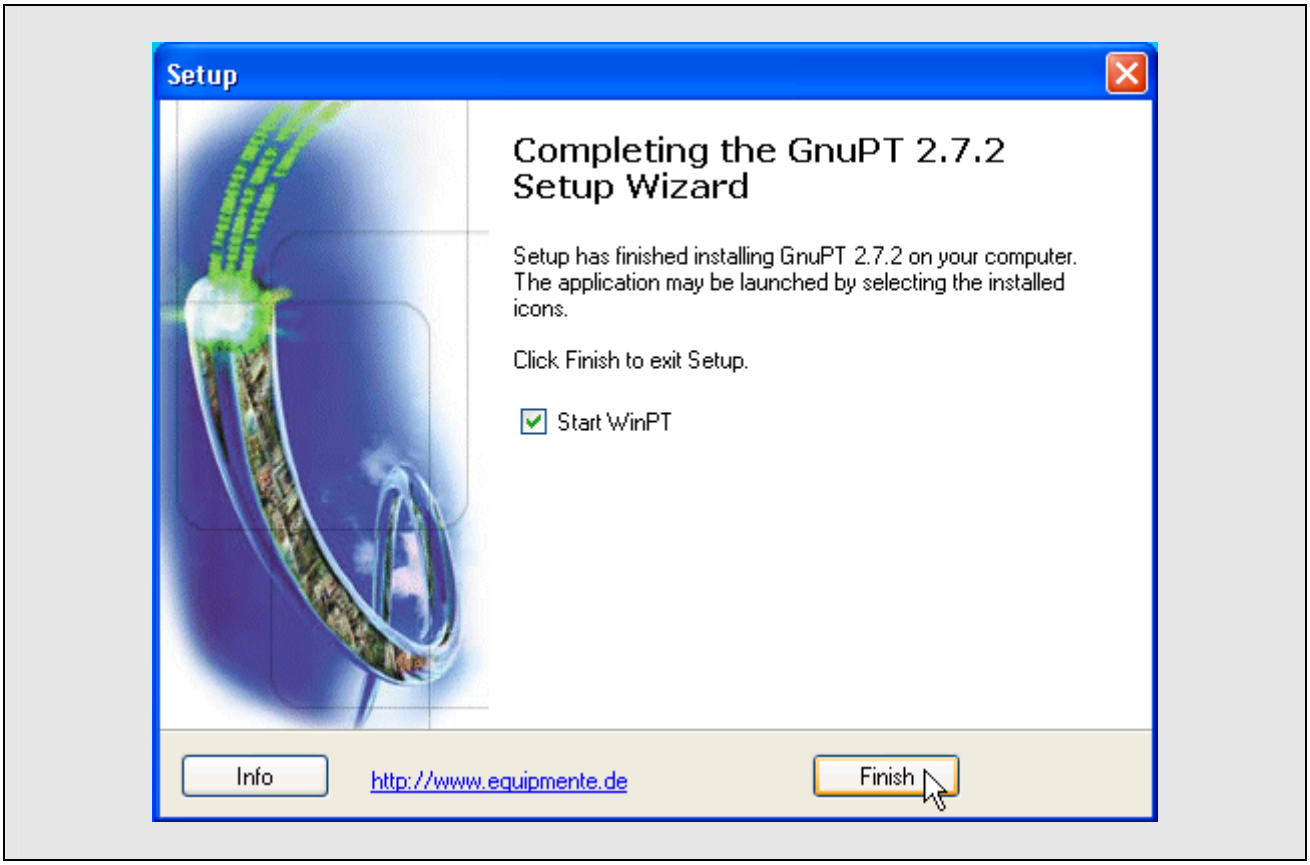
- Accept in the next two windows the pre-selected parameters
- Click **Next** in the first window and **Install** in the second one.
- The WinPT application will then be installed.





Complete the installation

- Keep the selected box '**Start WinPT**'.
- Press the **Finish** button

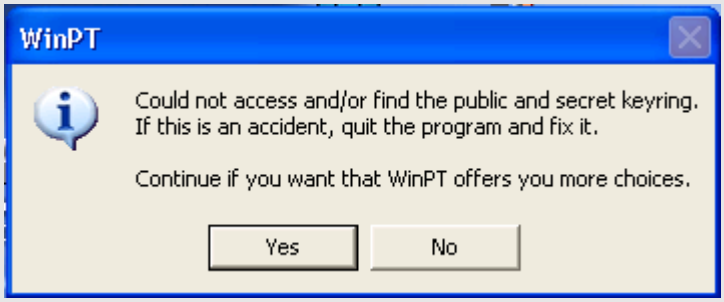


- After this, the wizard program finishes the WinPT installation. The application has been installed and the WinPT configuration starts immediately without an interrupt.

3.2 WinPT Configuration

- Immediate after the software installation it appears a small pop-up window with an error-message. You will get this information when the installer program doesn't find any key pair on your PC. **This message is normal.**

- Click **Yes** to continue



Look ahead
If you don't get this window, probably the installer program has detected an already existing key pair on your PC and is trying to use these keys. This could occur, e.g. when in the past another cryptographic software based on PGP has been installed.

GnuPG Preferences

The next window shows you information about the different locations used by the application.

- Click **OK**

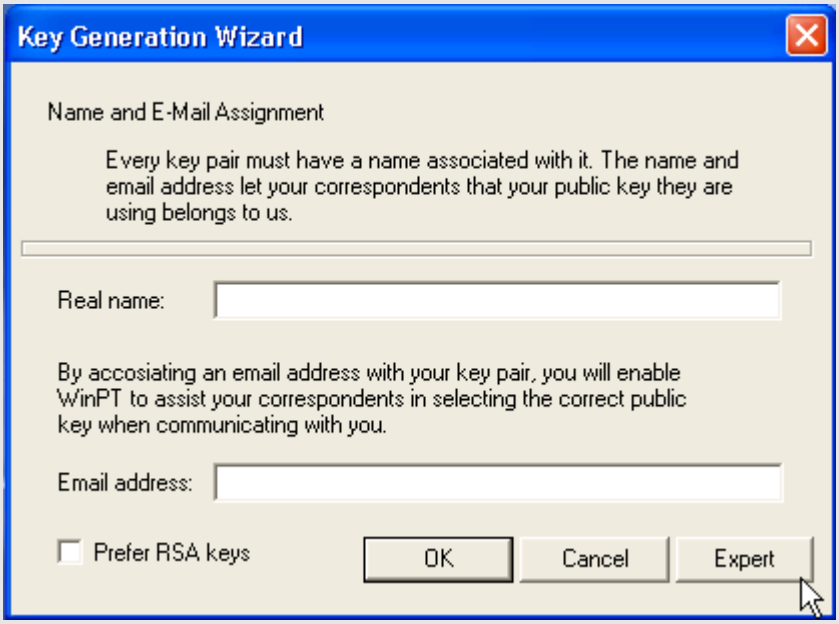
Key Generation (I)

- Select the first line '**Generate a GnuPG key pair**' in the following window
- Click **OK** to continue

Key Generation (II)

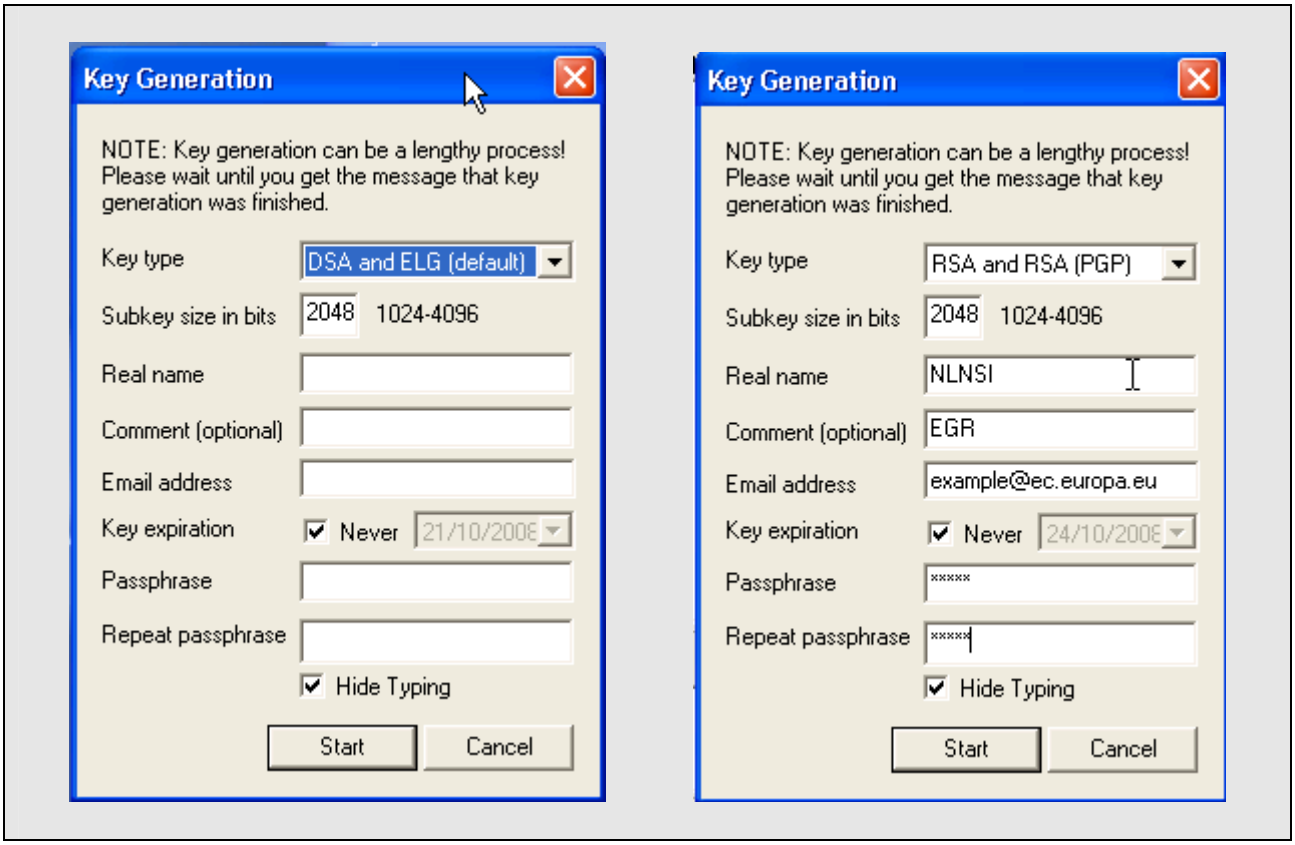
- In the following window "Key Generation Wizard" you will be prompted for additional information in order to generate a new key pair.

- Select **Expert**



Key Generation (III)

- It appears a window with predefined parameters (picture on the left side). Please enter the following for the different options.



- *Key type*
  Change the key type and select as key "RSA and RSA (PGP)".

- *Subkey size in bits*
  Keep the predefined parameter.

- *Real name*
  The name consists of two parts. The first two alphabetic characters are the code of your country following the standard ISO 3166-1 alpha2, e.g. NL for Netherlands.
  The remaining three characters are reserved either for the national statistical institutes (NSI) or the national central banks (NCB).
  The example in the right picture "NLNSI" is the abbreviation for the national statistical institute of Netherlands.

- *Comment*
  Enter as comment EGR.

- *Email address*
  You have to enter an email address. However you can choose any convenient address you want.

- *Key expiration*
  Keep the predefined parameter.

- *Passphrase*
  You have to enter a password containing at least eight alphanumerical characters. You can use any character you want.

  Please keep the passphrase in safe custody because it is needed later in order to decrypt among other things coded files from Eurostat

Key Generation (IV)

- You will see a new task starting in the window 'Key Generation - Process Dialog'
- When the key generation is finished, a small pop-up window will appear.
- Choose **OK.**

- When the installation is finished correct, it is not necessary to reboot the computer.

4.Export of Public Key for Eurostat

Check that WinPT is running

- After the installation, there should be a key icon both on your desktop and on your taskbar.

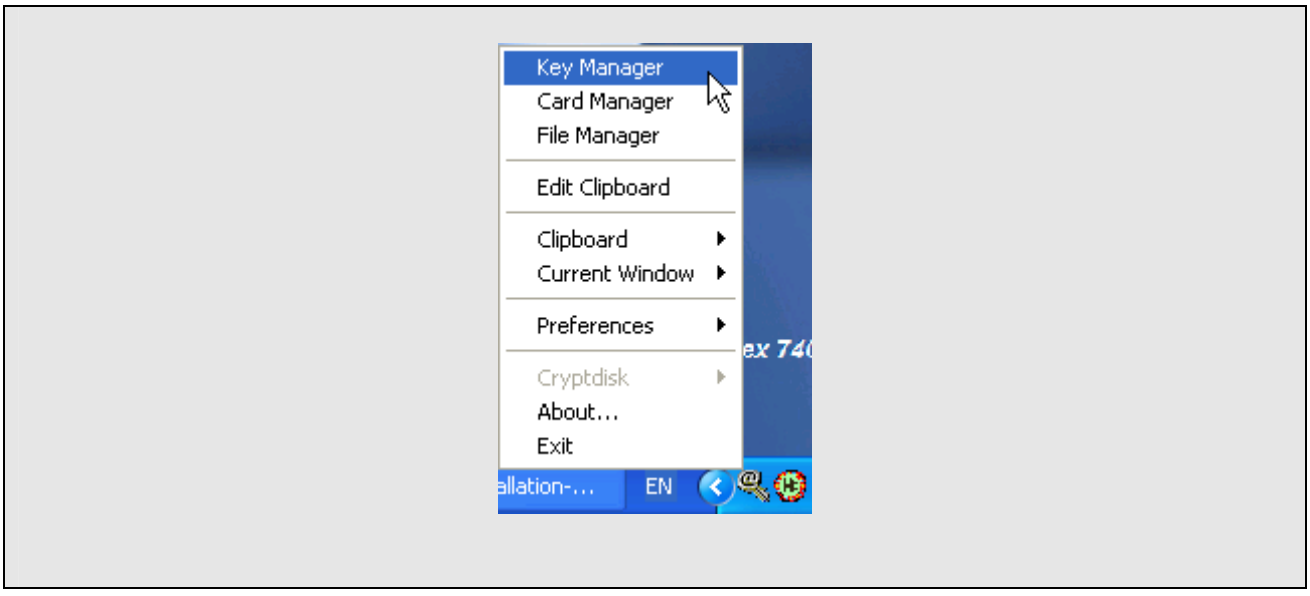
- The WinPT program is then running.

Look ahead
If you try to double click the icon on the desktop you receive an error message that the program is already running.

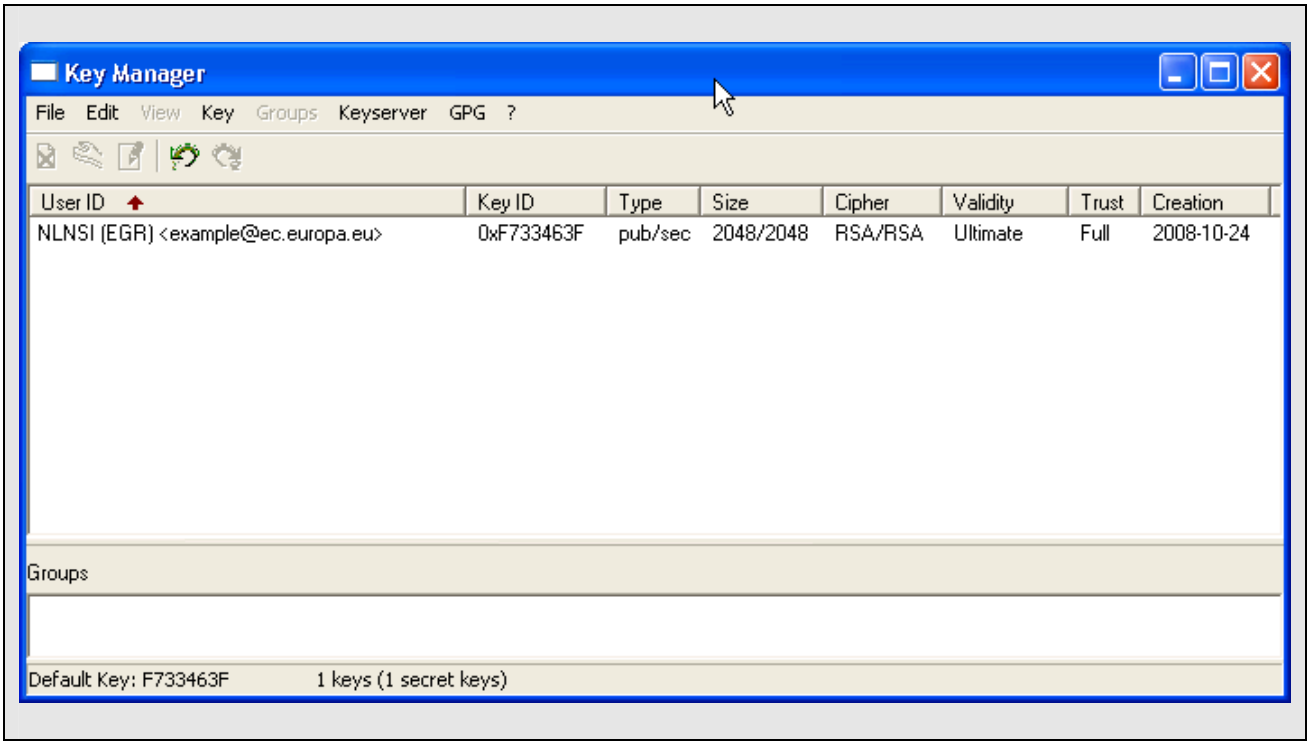
4.1 Key Export

- Open with the right mouse button the little key icon on the taskbar.

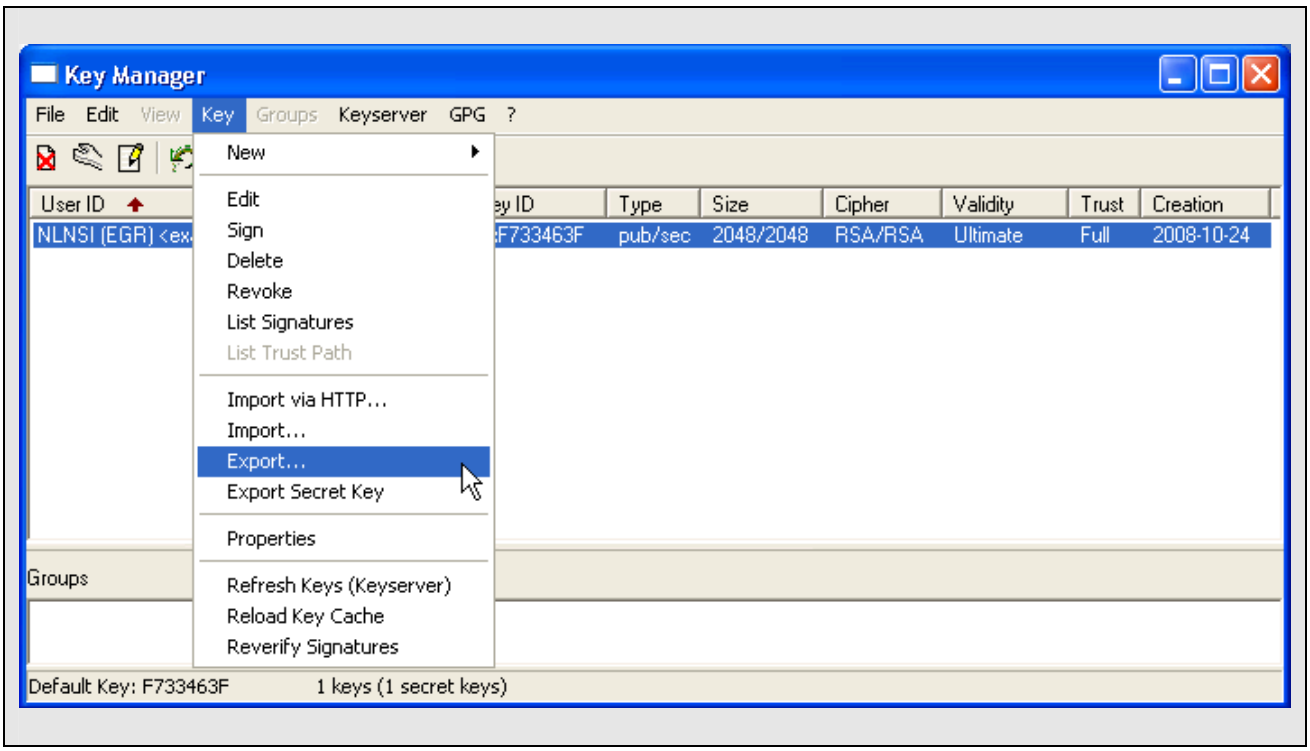
- In the WinPT menu, which then appears, click **Key Manager.**



- In the key manager window you will find information about your already created key pair (see Key Generation on page 16).

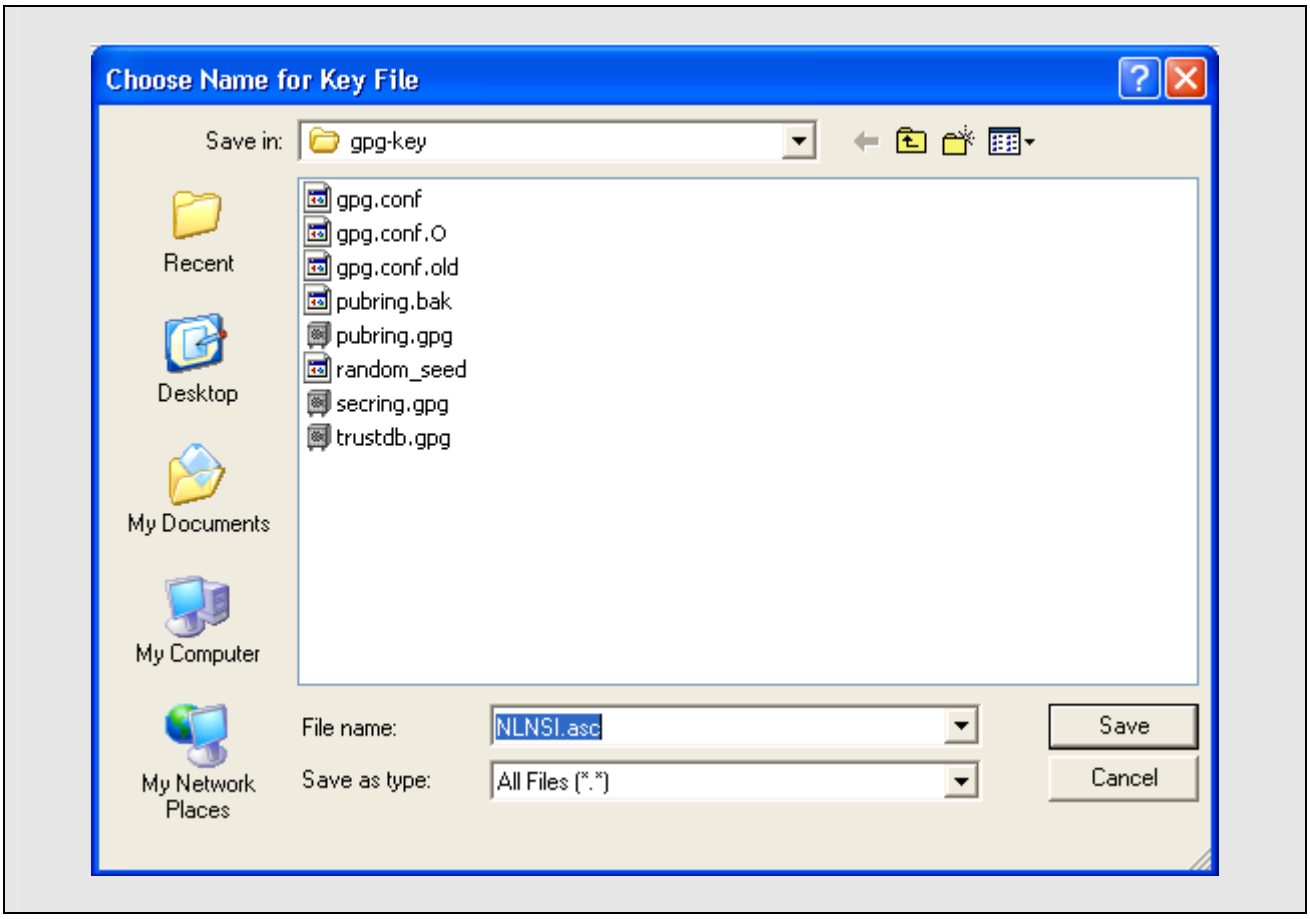


- Within the Key Manager menu select the **Key** option and then click on **Export.**

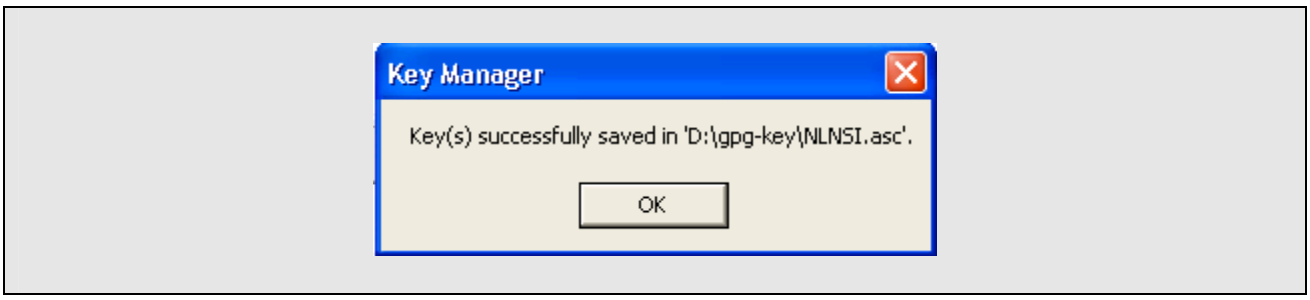


- It appears a window in which you have to enter the directory place of your public key file. We recommend storing the file in the same directory where your key pair has been placed.
  The file name has the form xxxxxxxxx.asc (see the example in the below-mentioned window).

- Click on **Save.**



- Finally you will be informed that the file has been stored successfully.
- Click **OK** to continue



4.2 Send public key to Eurostat

In order to make your public key available to Eurostat take the file (xxxxxxxxx.asc), annex it as attachment to an email and send it to Eurostat.

5. Decrypt data files received from Eurostat

After the WinPT / GnuPG software was installed and your public key has been successfully imported into Eurostat WinPT/ GnuPG application you will receive coded files.

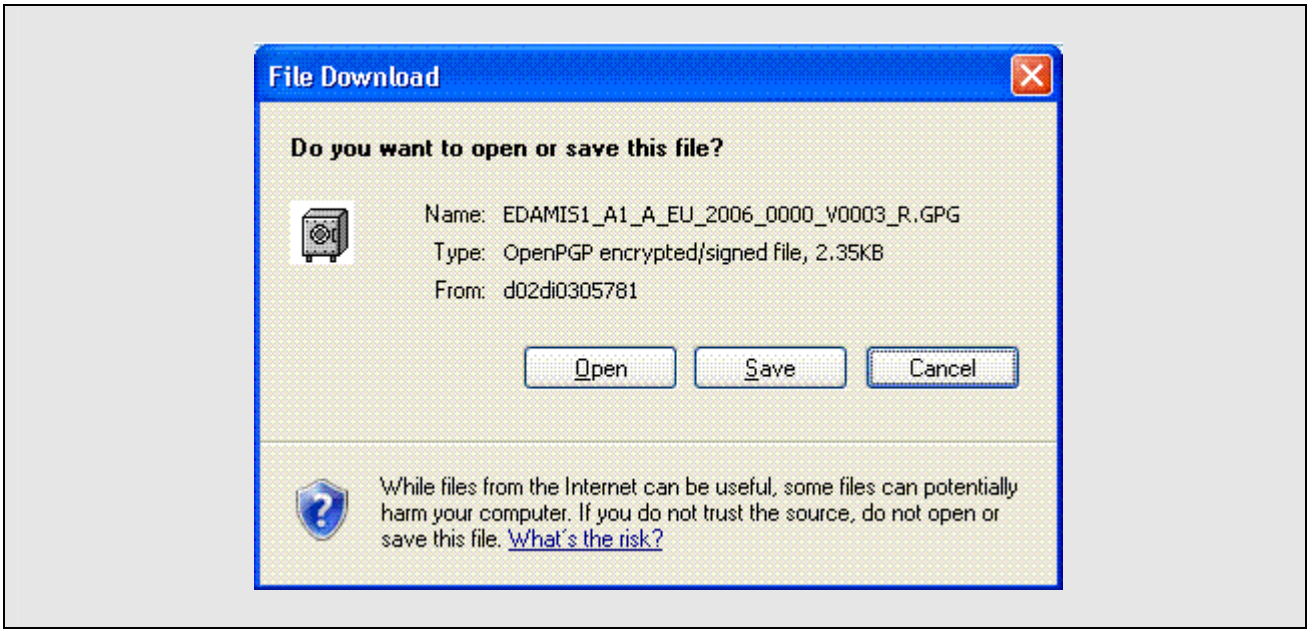
Kindly note the following points:

- The decrypted file has always as extension the format ".gpg".
- The decryption software takes the input file, decrypts it and creates a new output file without the extension ".gpg".
- The decryption software decompresses the input data.

Download coded file

- Inside eDAMIS Web Application download the coded file you have received from Eurostat.

- Click **Save**
  Store it on any convenient directory on your PC / server.

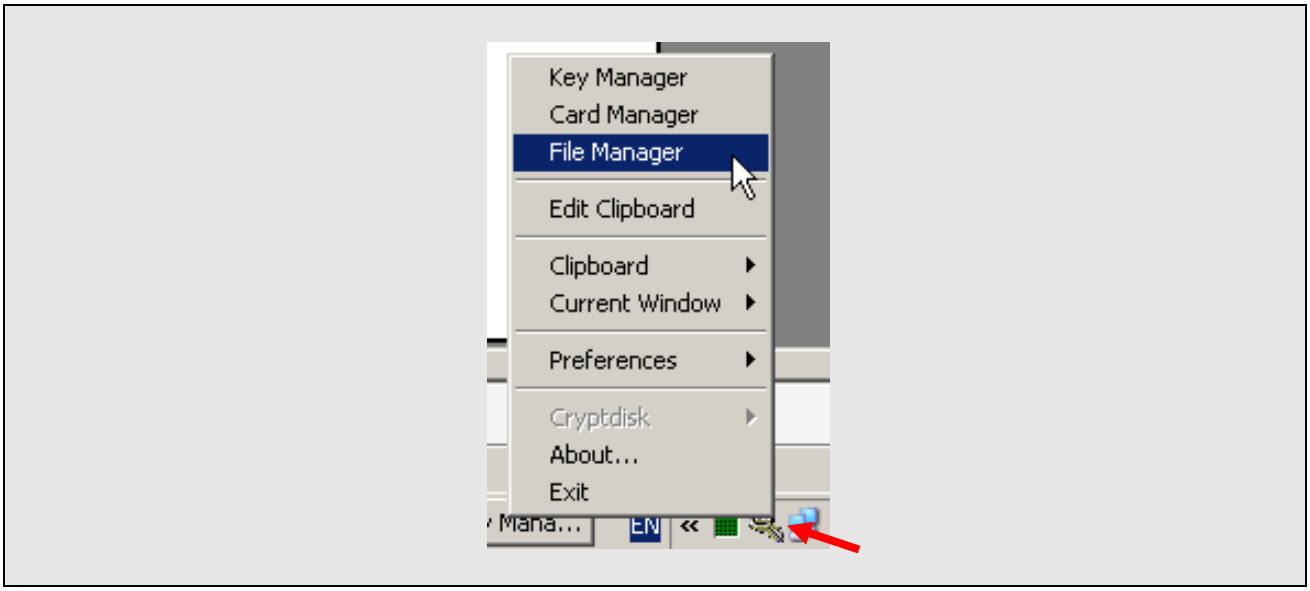


Open Windows Explorer

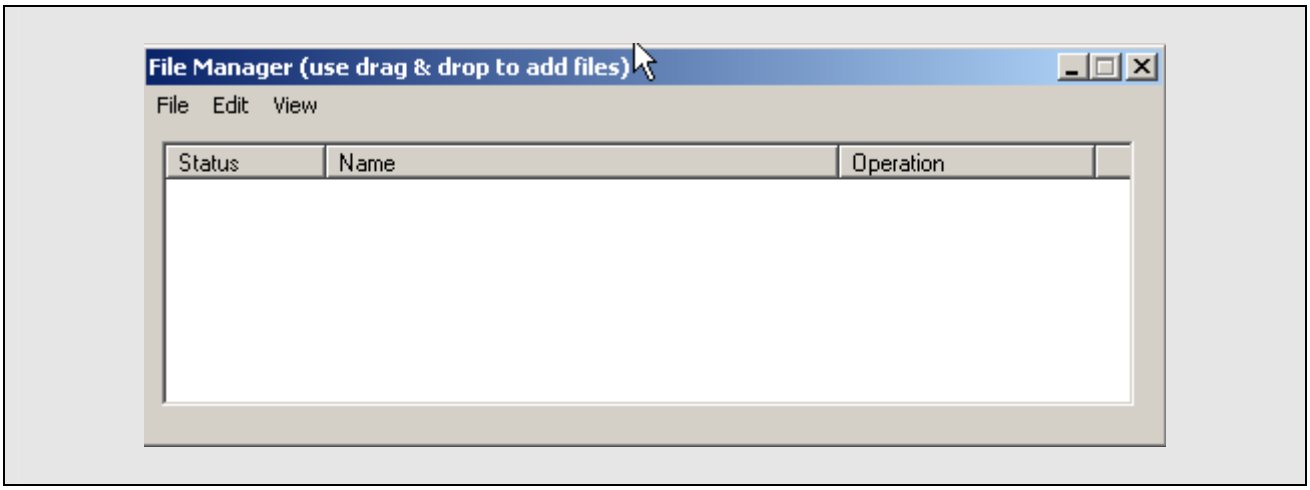
- Open the directory where the coded input file is stored.

Open WinPT File Manager

- Click with the right mouse button the little key icon on the task bar (see red arrow).
- On the WinPT menu, which then appears, click **File Manager.**

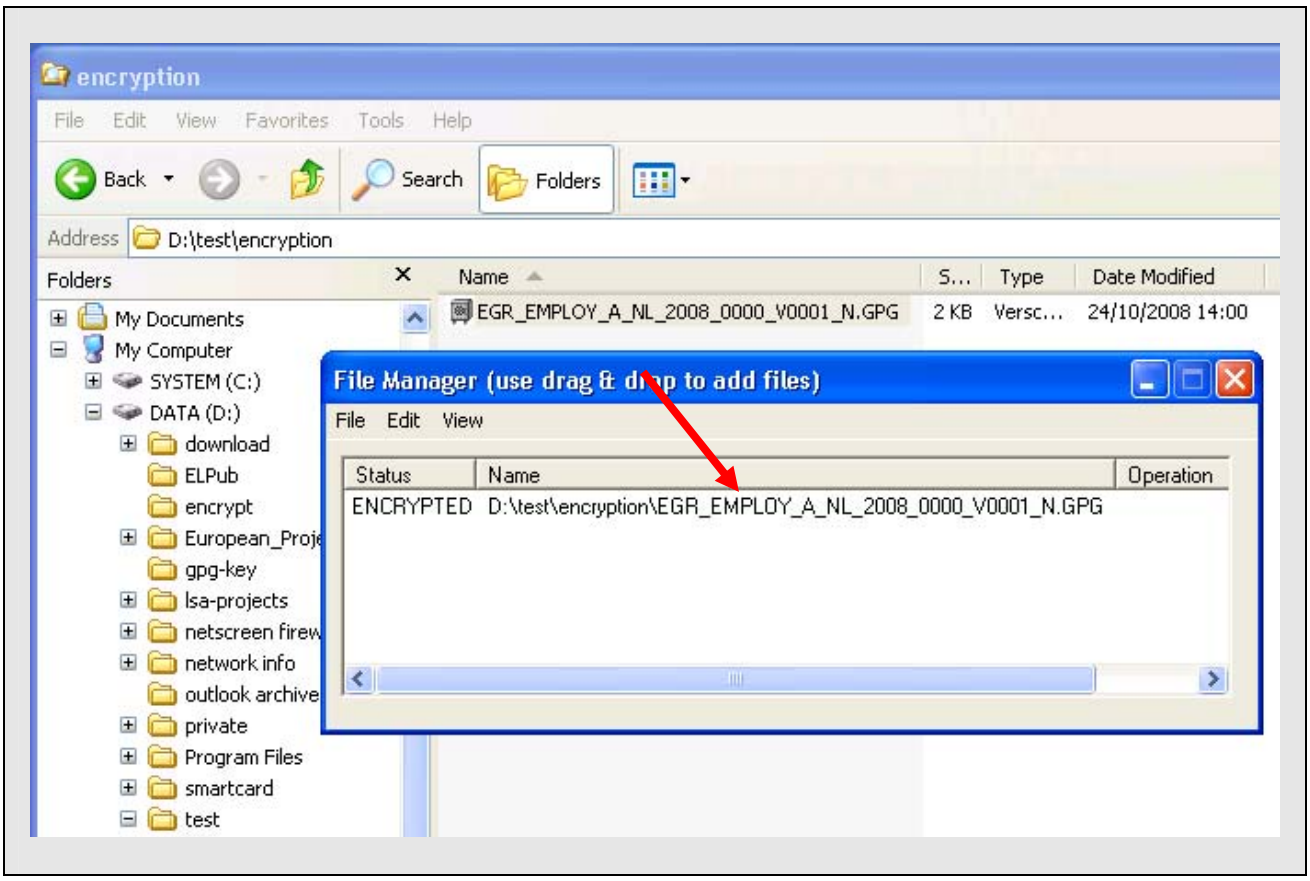


- It opens the File Manager window of WinPT.



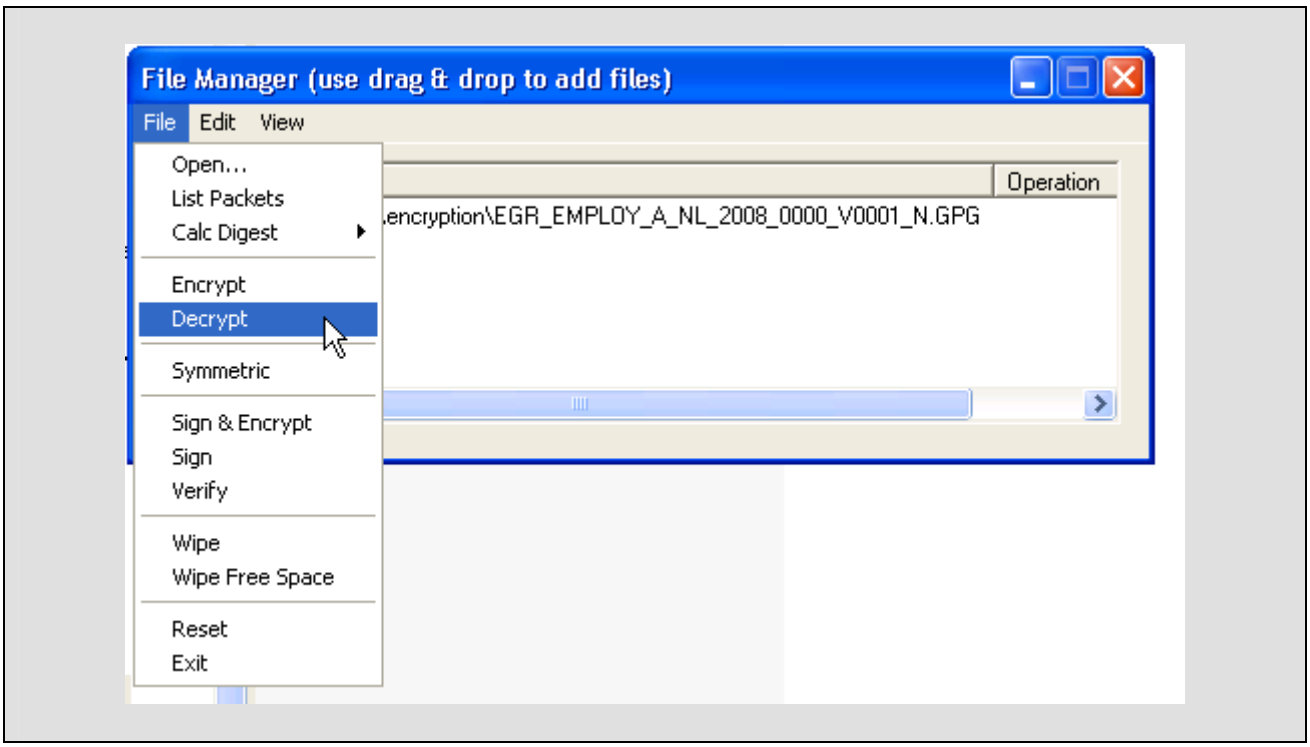
Decrypting the file (I)

- In order to decrypt the input file, simply drag & drop it from the Explorer window to the WinPT File Manager window.



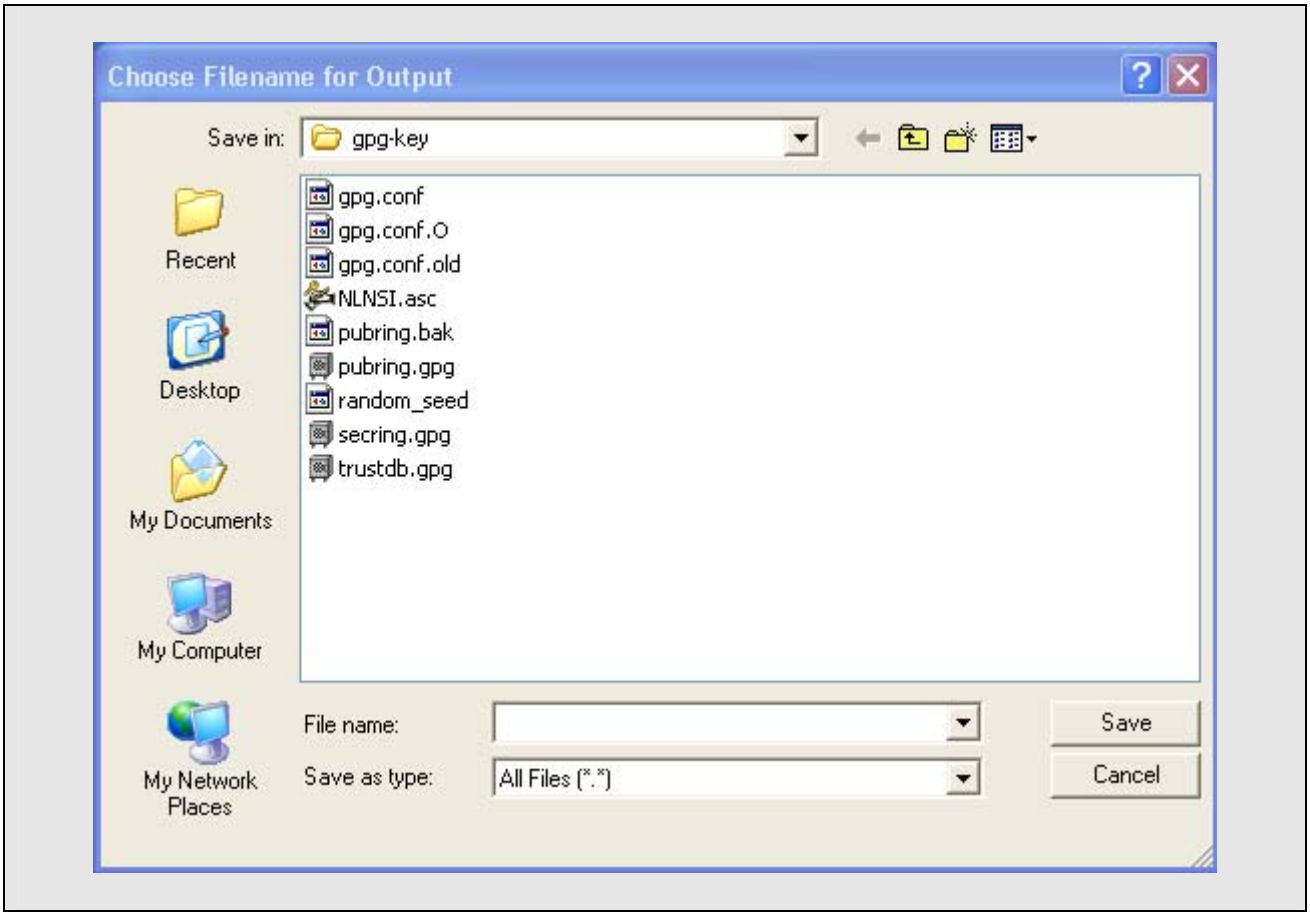
Decrypting the file (II)

- Select within the File Manager window the coded file.
- Open the **File** menu and click on **Decrypt**



Decrypting the file (III)

- It appears a window showing your GnuPG home directory, i.e. it contains the key files which were created by the installation process of WinPT / GnuPG.

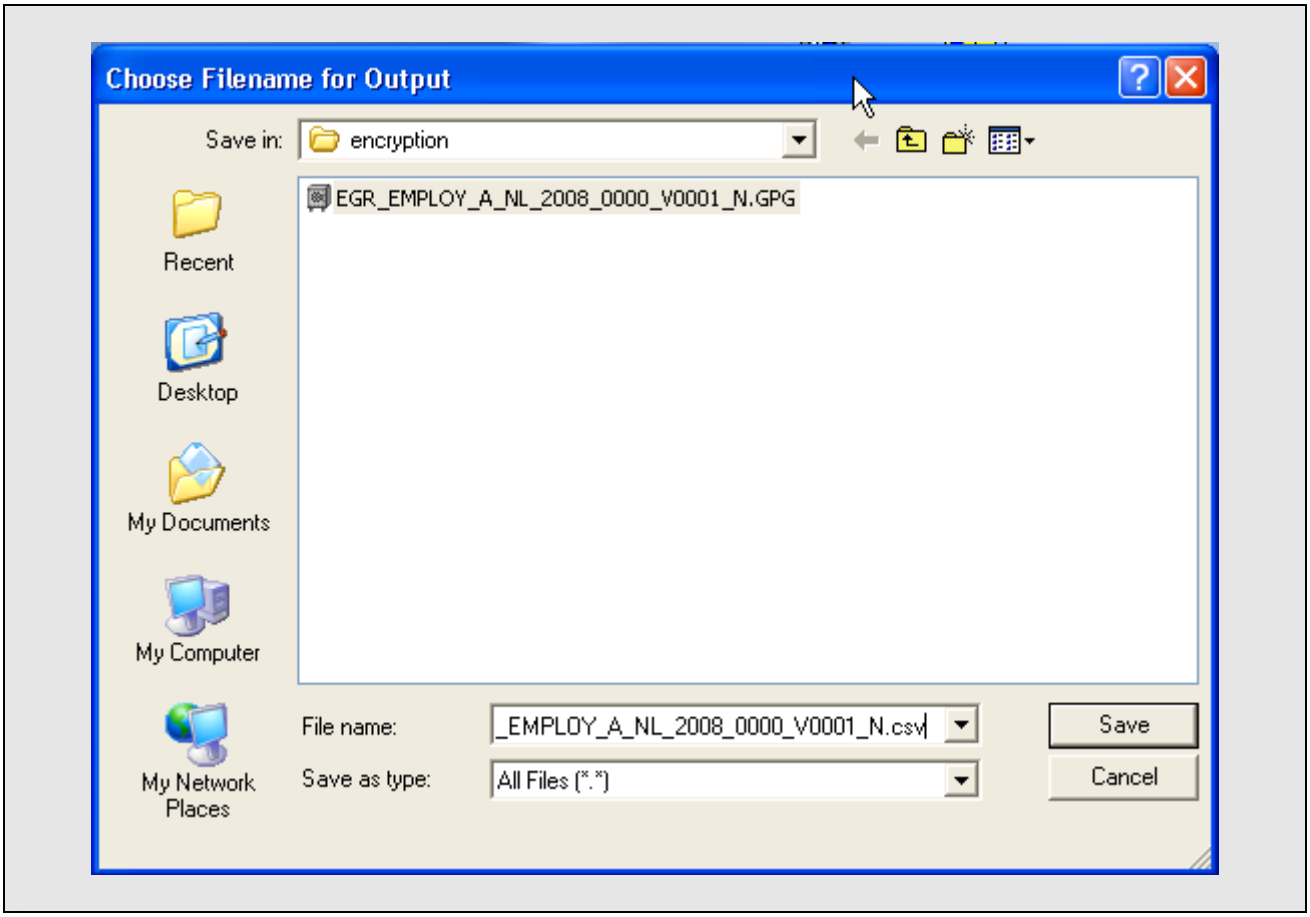


Decrypting the file (IV)

- Switch to any convenient directory where you want to store the decrypted file
- enter a valid file name in the form "new file-name.csv"

Look ahead

*The encrypted file you have received has the format "file-name.gpg". During the decryption process, the application GnuPG takes the whole name of the file, removes the extension ".gpg" and creates a new file composed of the remaining part of the former name. However this name does not have a valid extension for Windows. In order to avoid a problem you have to use as file extension the format "**.csv**". At the moment Eurostat uses this file format.*



Decrypting the file (V)

- In the following window enter the passphrase which you have created during the WinPT/GnuPG installation.

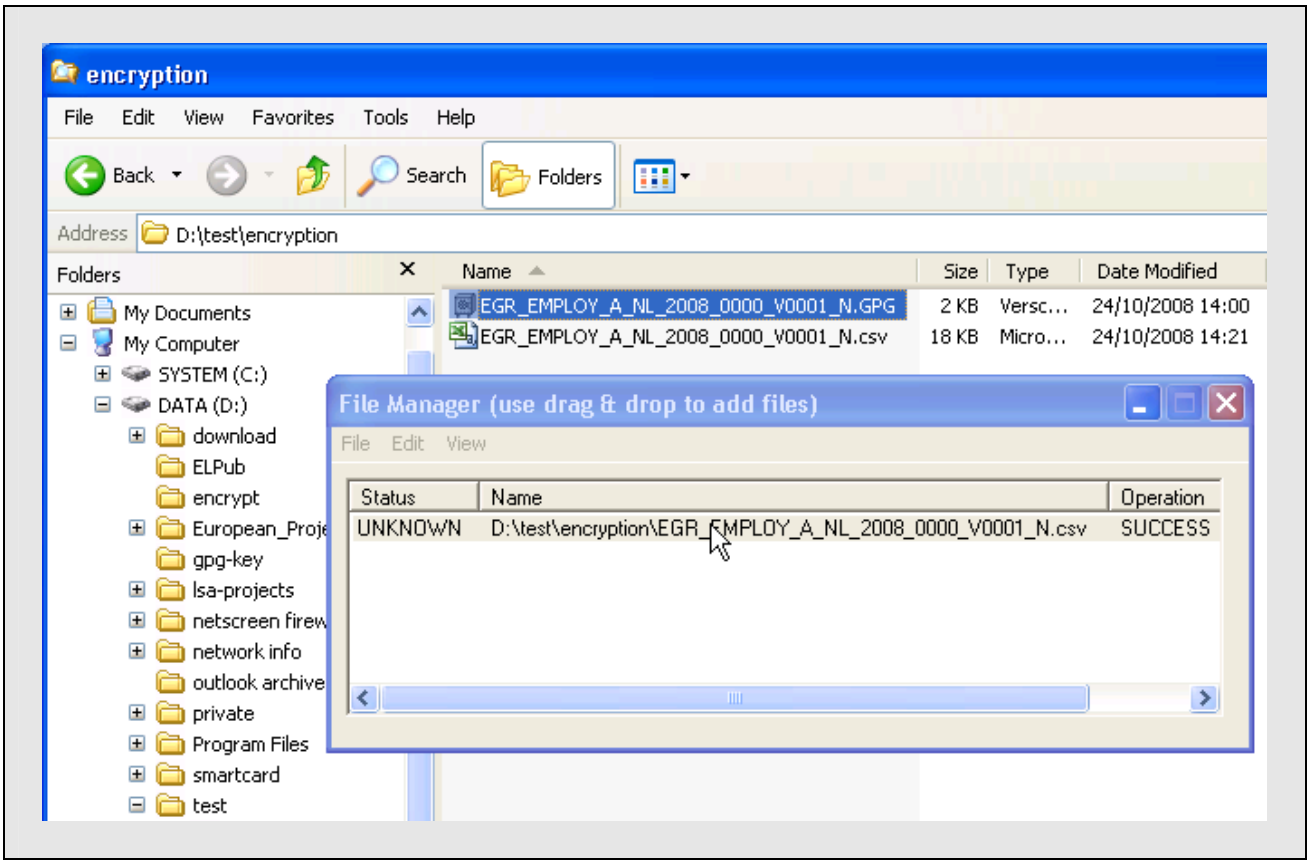
- Click **OK**

Decrypting the file (VI)

- After the decryption process is finished it appears again the File Manager window.

- When the decryption process succeeds, it appears the **SUCCESS** message in the **Operation** field. In the **Status** field the entry changes from **ENCRYPTED** to **UNKNOWN**.

- The new decrypted file is then stored in the directory you have selected.



6. Short Documentation

If you have used the given parameters for installing the WinPT application you will find below-mentioned a list with helpful information. These settings refer to Window XP.

- Standard folder — C:\Documents and Settings\username\GnuPT
  - -> GnuPG executable — GPG
  - -> Language Support — Locale
  - -> WinPT executable — WPT
- Registry Keys — HKEY_Current_User \ Software \
  - -> GNU — GNU
  - -> WinPT — WinPT
- Registry Keys — HKEY_Local_Machine \ Software \
  - -> GNU — GNU
- Program for uninstalling WinPT — C:\Documents and Settings\username\GnuPT\unins000.exe

7. Support

If you have questions or you need support concerning software installation / configuration, export of the public key or file decryption, please contact your partner in Eurostat. He / she will respond to your question.