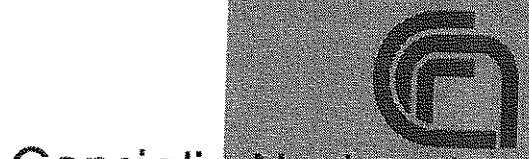


Consiglio Nazionale delle Ricerche

The INDUCE web site: Encrypting and decrypting documents

Massimo Martinelli

B4-52
dic-2001

Project N° BE 97 - 4057
Contract N° BRPR - CT98 - 805

WP2 State-of-the-Art and definition of the Industrial requirements

WP2.1 State-of-the-Art

WP2.1.4 Monitoring

Title	**The INDUCE web site:** Encrypting and decrypting documents
Document Type	*Contribution Report*
Summary	In order to improve the security level for accessing the web site a new procedure has been developed for encrypting files to be processed. This procedure can also be used to transfer files securely using internet connections, as email, ftp or http. In this technical note we describe this procedure mainly putting in evidence the relation between encrypting/decrypting files and uploading/downloading documents.
Keywords	Web Site, Encryption, Decryption, PGP, Upload.
Internal Reference	IEI-TR-07
Prepared by	M. Martinelli

TC BAe	**WPC** CESI	**PC**

The PGP software tool

The PGP freeware program (Pretty Good Privacy) has been chosen as the basic tool to perform file encryption and decryption. This program can run under many platforms.
PGP package is downloadable at the following address:

http://www.pgpi.org/products/pgp/versions/freeware

The current version (7.03) has a *hot fix*, and then we need to download this file too.
In the following section, the procedure for Windows systems will be described, considering that for other systems it is very similar.

Software setup

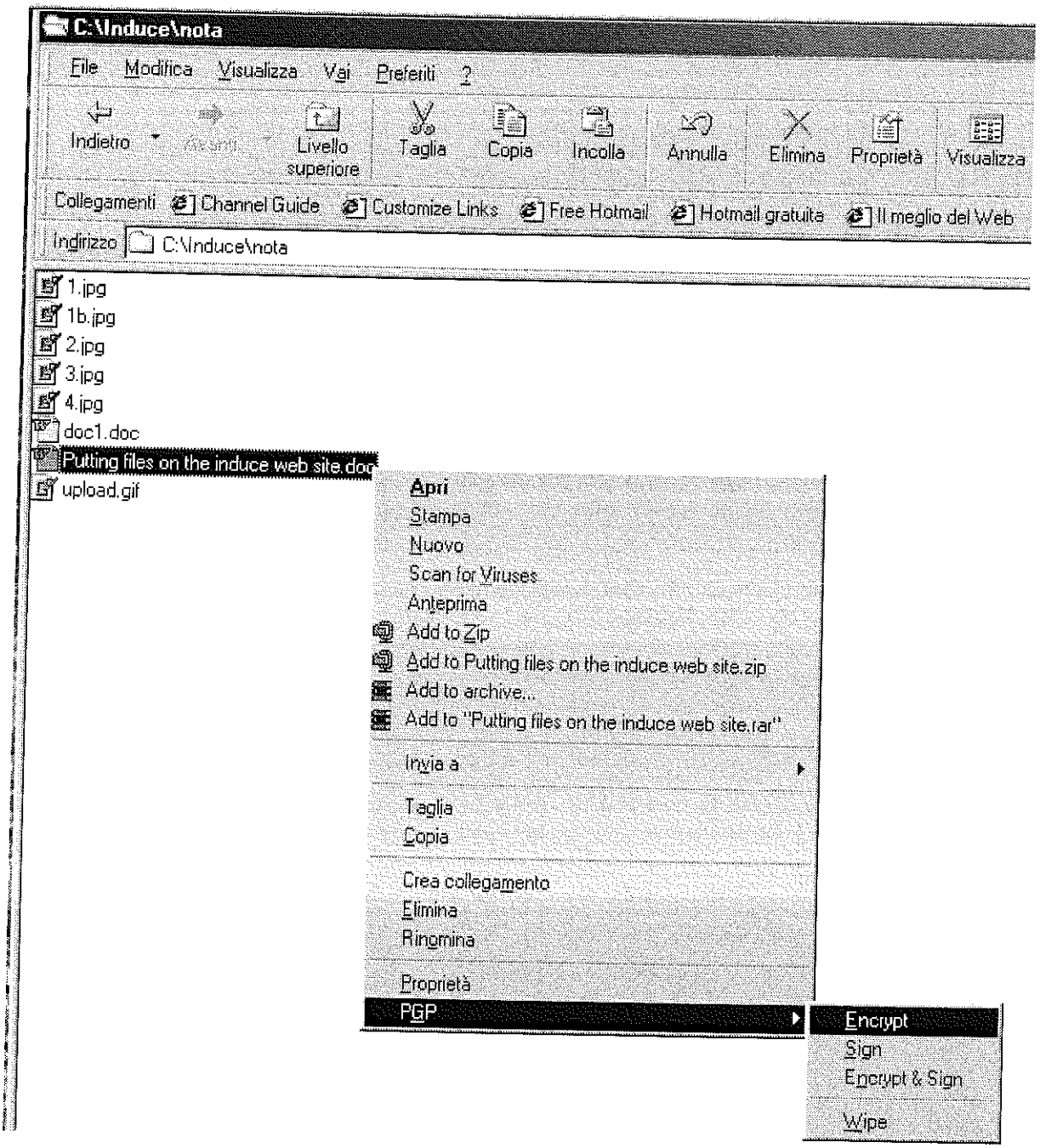
The installation procedure can be summarized as follows:

1) Unzip the application (PGPFW703.zip) in a temporary directory (e.g.: c:\tmp)
2) Launch the setup (PGPFreeware.7.0.3.exe)
3) Choose the following buttons: *Next*, *Yes*, *Next*, *No I'm a new user*, *Next*.
4) Select all the internet interfaces
5) Digit a password
6) Instead of "Yes, I want to reboot windows" select "No".
7) Decrypt the PGPfreeware703Hotfix1.zip file in a temporary directory (e.g.: c:\tmp)
8) Run the PGPhotfix.exe program
9) Reboot your system.

Encrypting files

The procedure for encrypting a file can be summarized as follows:

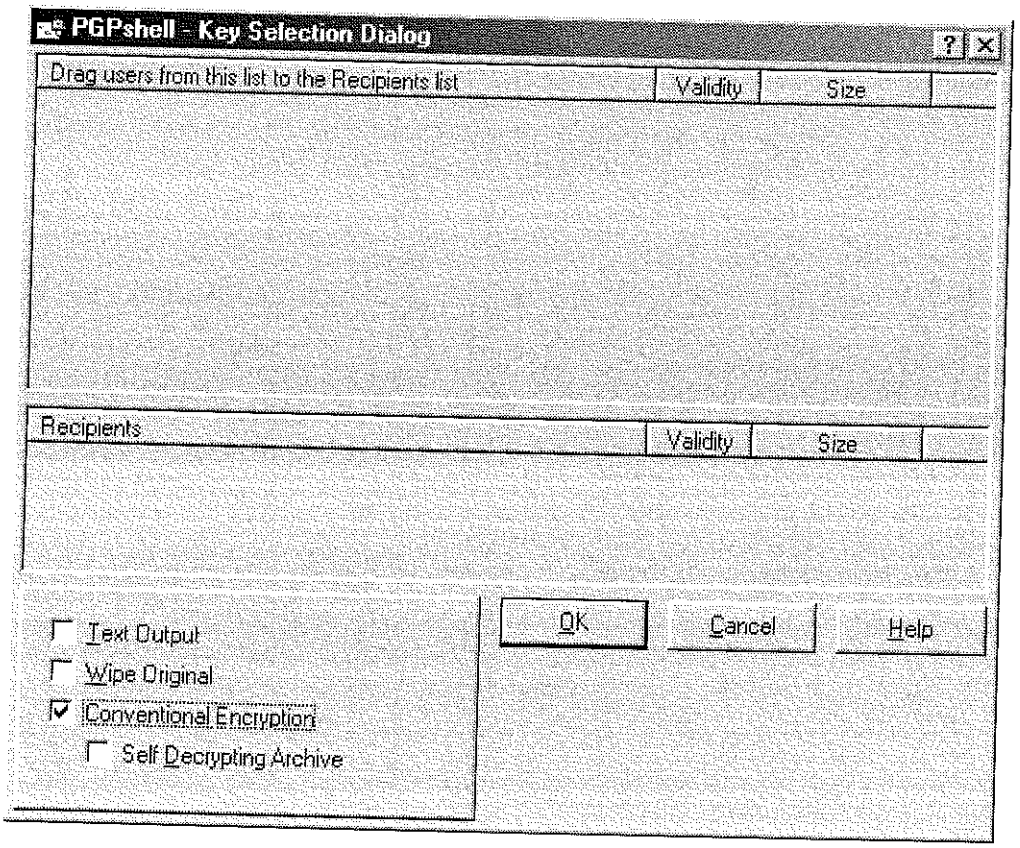
1) Select the files to be encrypted (e.g.: "Putting files on the induce web site.doc")
2) Click the *right button* of the mouse and choose "PGP"
3) Click on "Encrypt"



(A new window will be opened)

4) Choose "Conventional encryption"

5) Click the "Ok" button

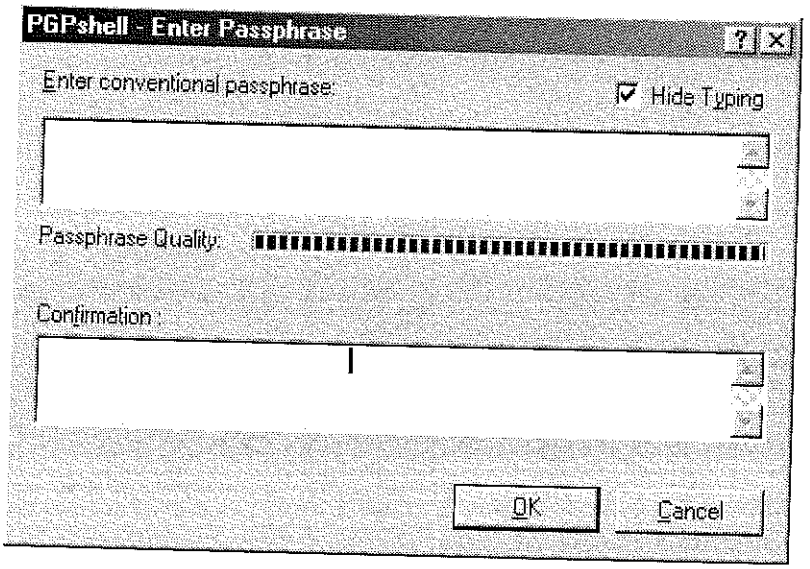


(A new window will be opened)

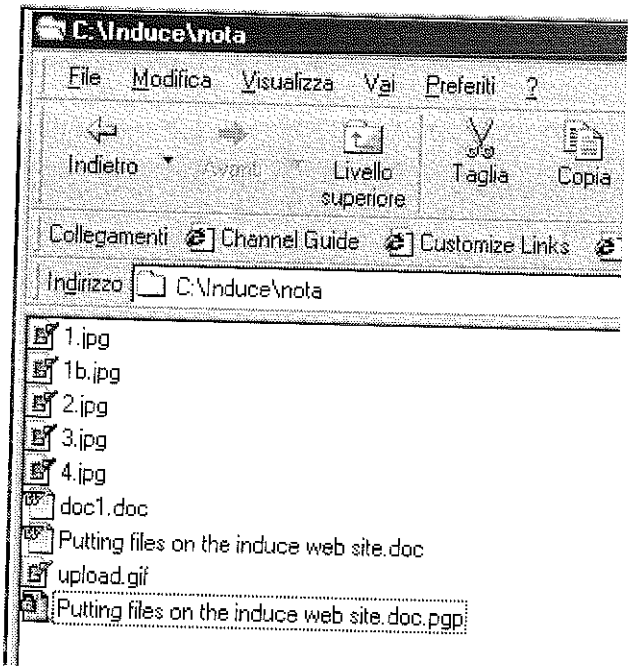
6) Enter a password in the "Enter conventional passphrase" field

7) Reenter the same password on the "Confirmation" field

8) Click the "Ok" button



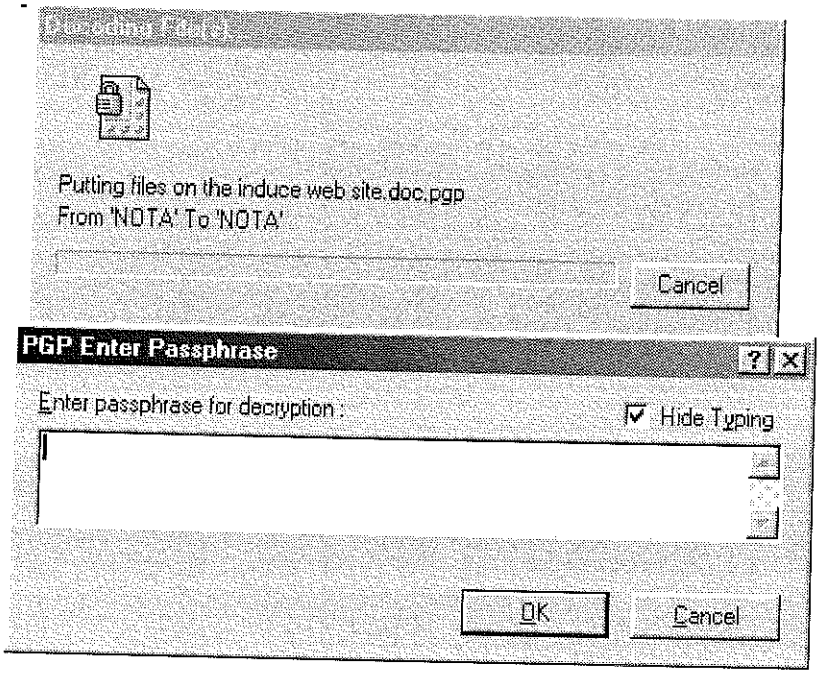
The encrypted file "Putting files on the induce web site.doc.pgp" has been created.



Decrypting files

The procedure for decrypting a file is the following:

1) Double click the files to be decrypted (e.g.: "Putting files on the induce web site.doc.pgp")
2) Enter the password



The file has been decrypted.

Obviously, in this case both *parties* agree on the private key and they use that key for encryption and decryption.

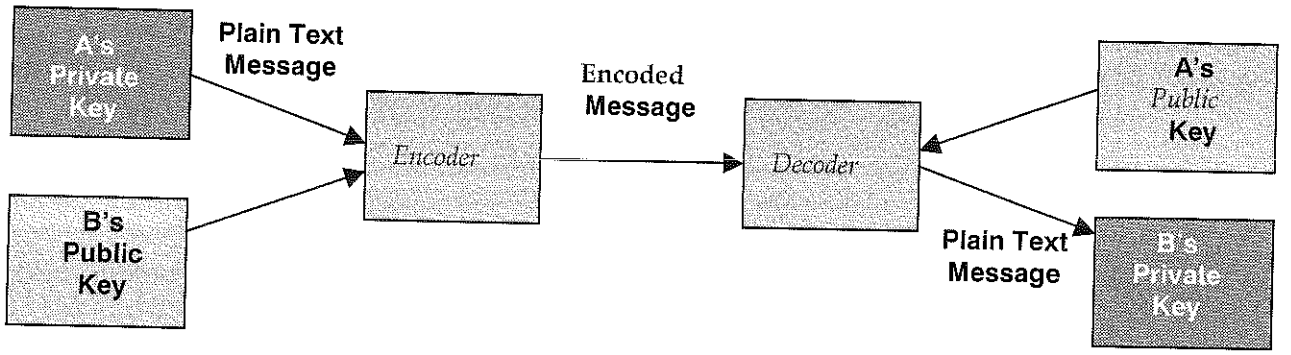
Other possible uses of PGP

Some interest have also other possible uses of PGP:

- partner-to-partner private communication and
- document personal authentication.

Partner-to-Partner private communication (Asymmetric keys)

Exchanging files *privately* between two partners is possible using a couple of passwords for each person, a public and a private one (*asymmetric keys*).
A person "A" can encrypt a file that only "B" is able to read using his private key and the public key of "B"; "B" can decrypt the file that "A" sends him using his private key and the public key of "A" (see the following scheme).

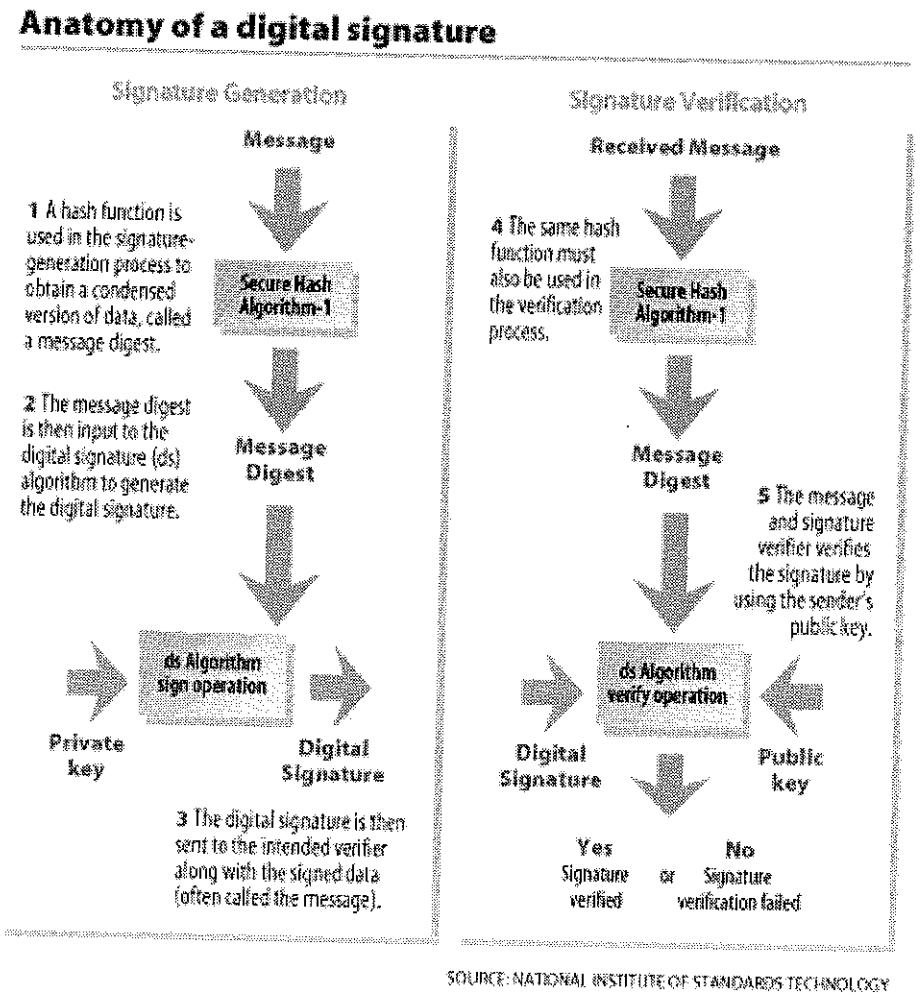


Document personal authentication (Digital Signature)

PGP can also be used for implementing a digital signature.

A user "A" can *sign a file* to guarantee other users that it is really the file written by him and that its content has not been altered.

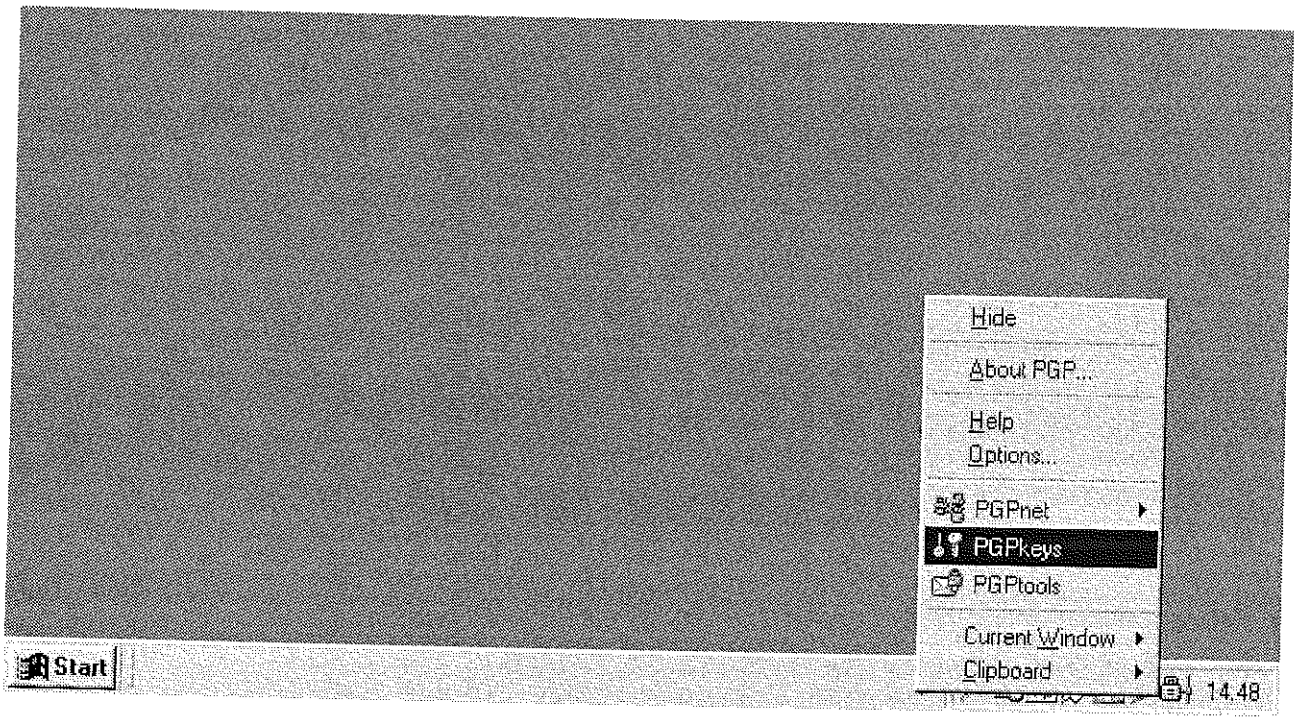
In the following scheme, the whole process is highlighted.



SOURCE: NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY

Exporting a Key

- Select the icon representing your key pair from the PGPkeys window



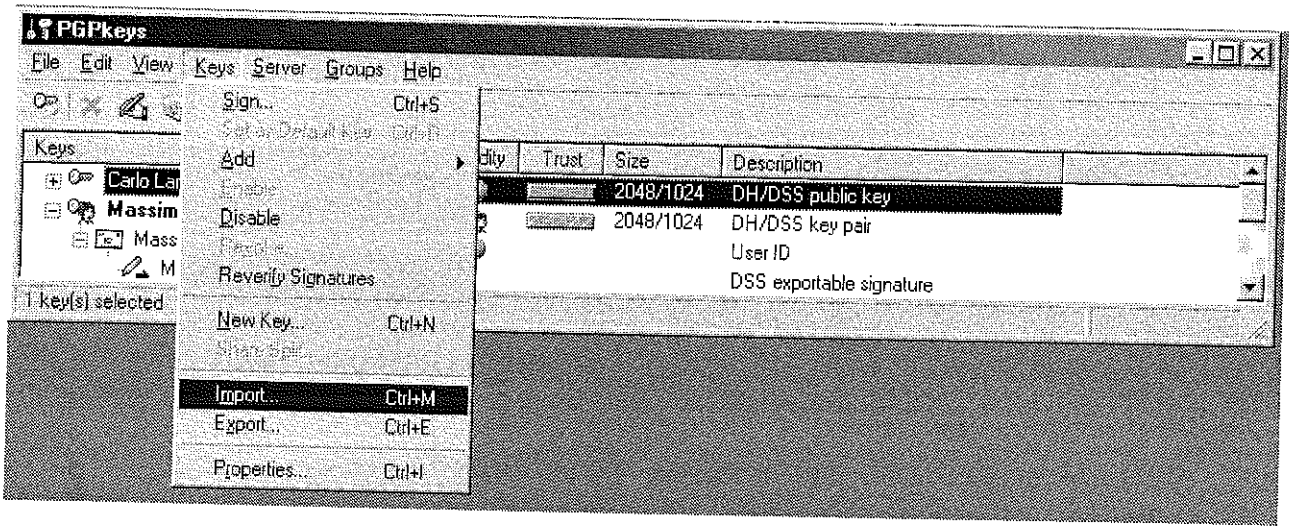
- Click Export from the Keys menu. Enter the name of the file to which you want to save the key.
- Drag the icon representing your key pair from the PGPkeys window and drop it where you want to save the key.
- Select the icon representing your key pair in the PGPkeys window, click Copy from the Edit menu and then click Paste to insert the key information into a text document.

Importing a Key

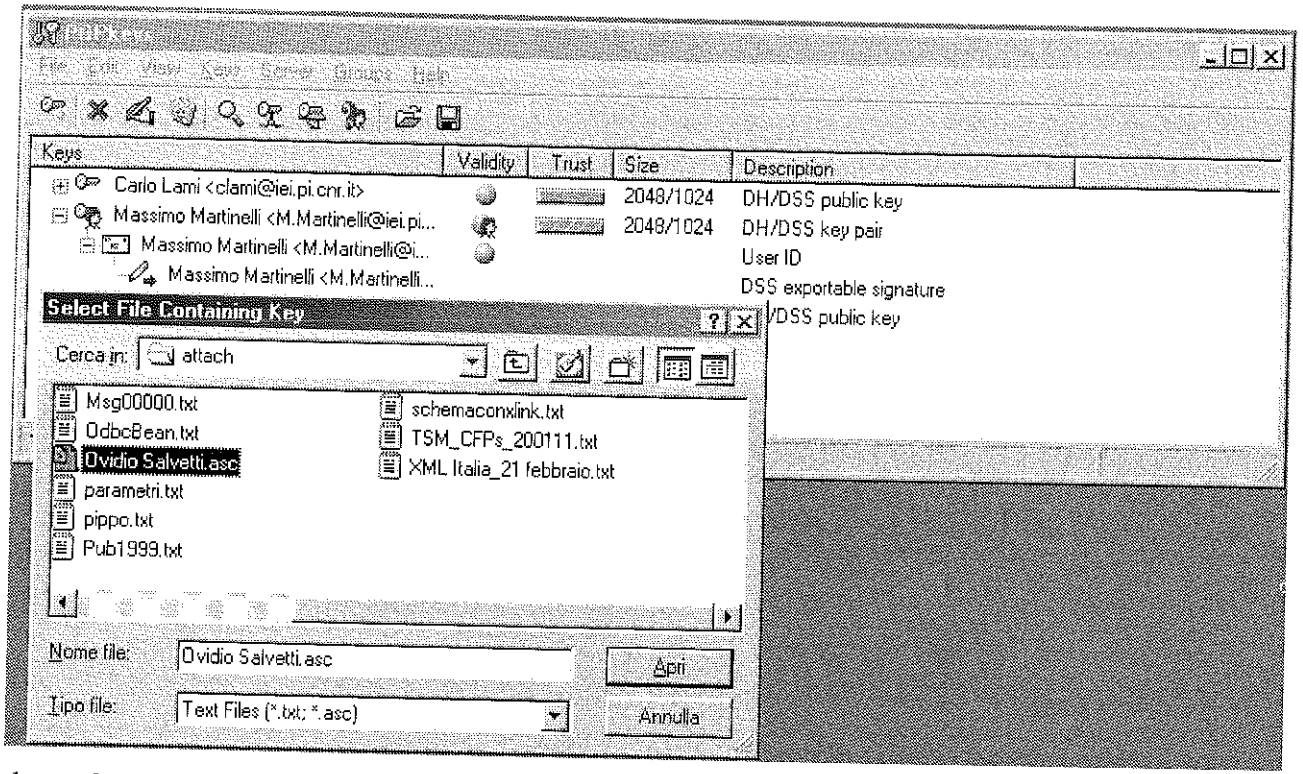
Suppose to import the Public key of 'Ovidio Salvetti'.

Click the "PGP" icon that appears at the right of the "Start" bar, then select "PGPkeys".

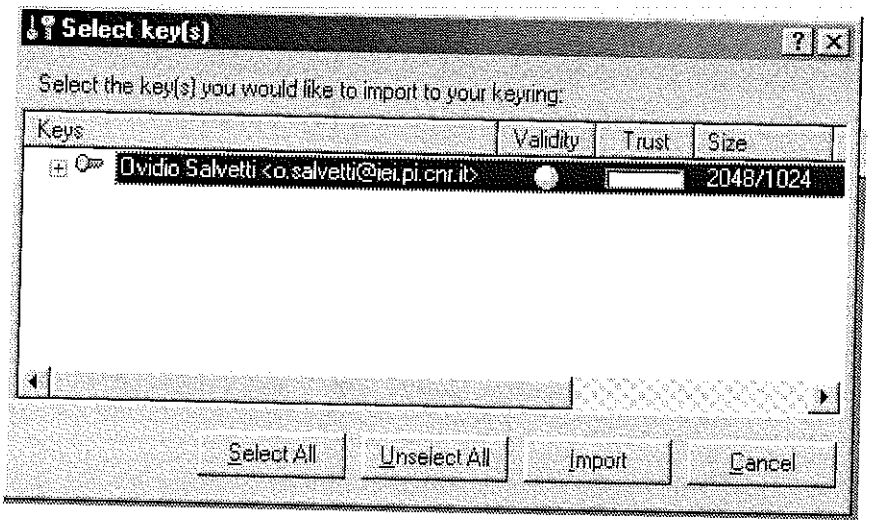
From the "Keys" menu select "Import"



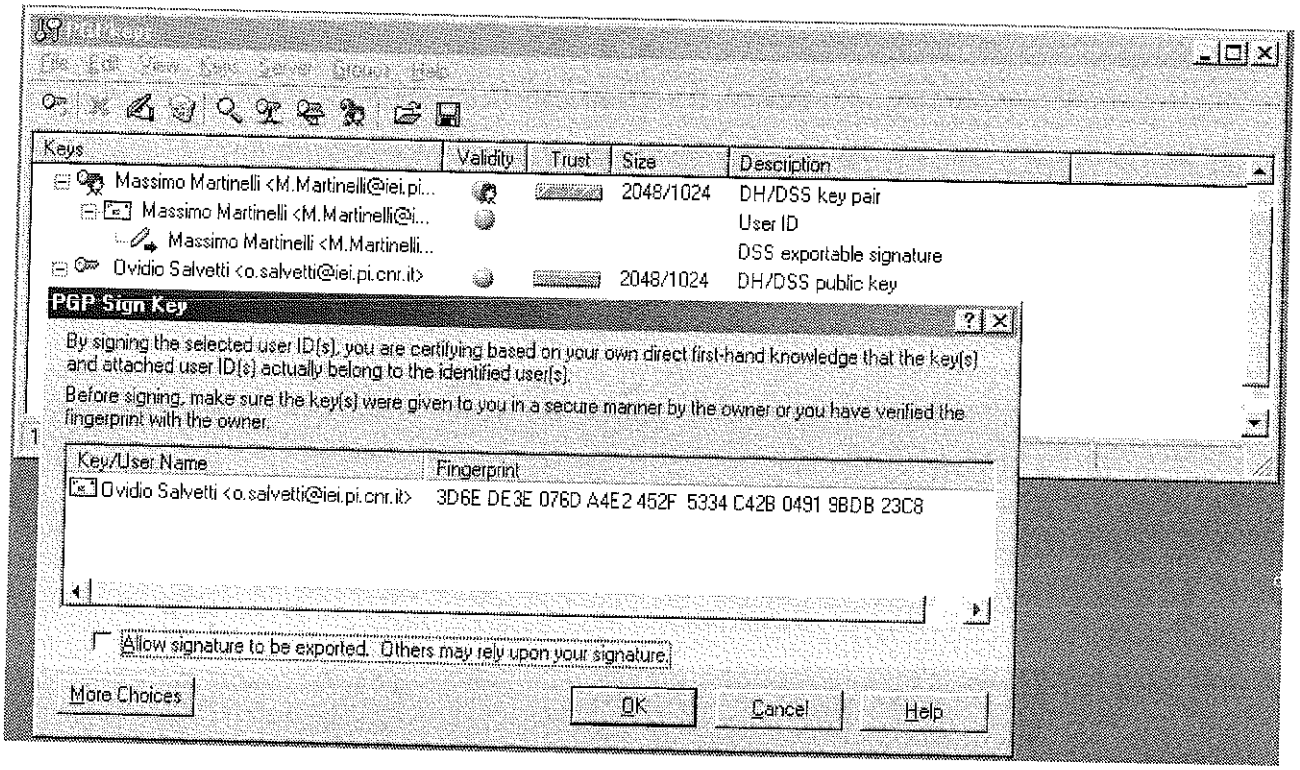
Supposing the key is included in the file "Ovidio Salvetti.asc" double click it



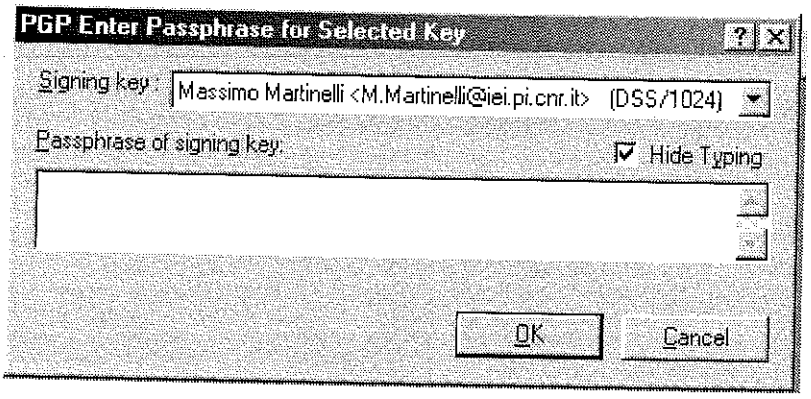
then select the "Import" button from the new window



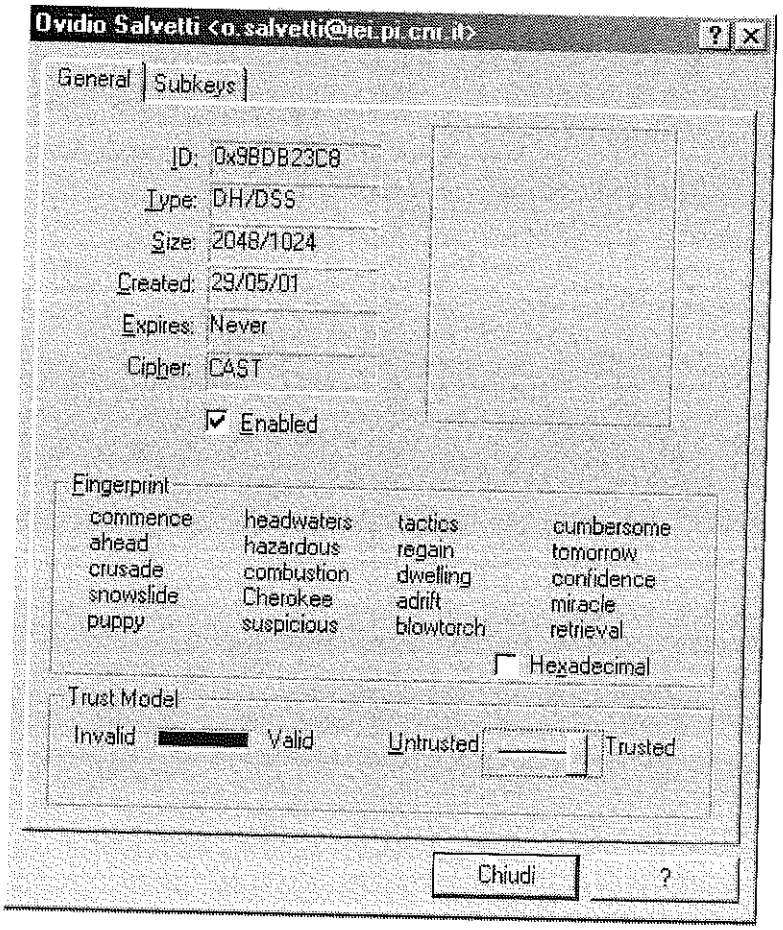
Sign the key by selecting the "Ovidio Salvetti <o.salvetti@iei.pi.cnr.it>" row with the right button of the mouse and then choose the OK button on the new window.



Now you must enter your password

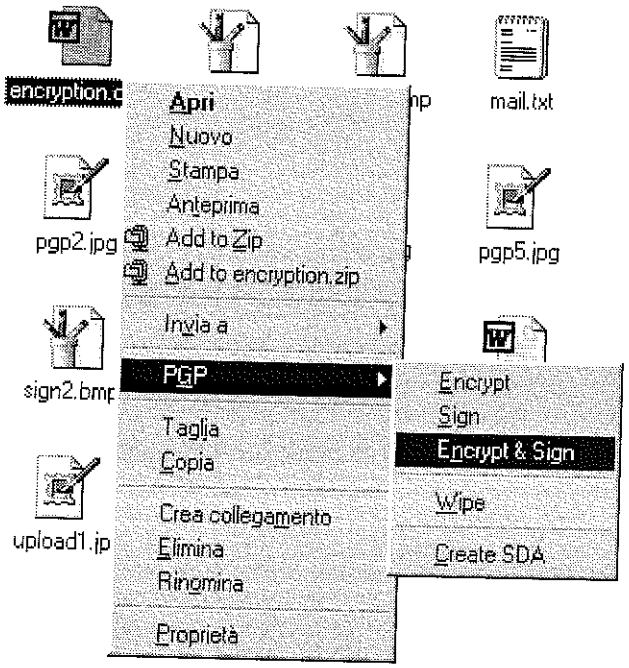


The last thing to do is to trust the key by selecting the "Ovidio Salvetti <o.salvetti@iei.pi.cnr.it>" row with the right button of the mouse and then select "Key Properties", moving the bar on the bottom right of the new window from "Untrusted" to "Trusted"

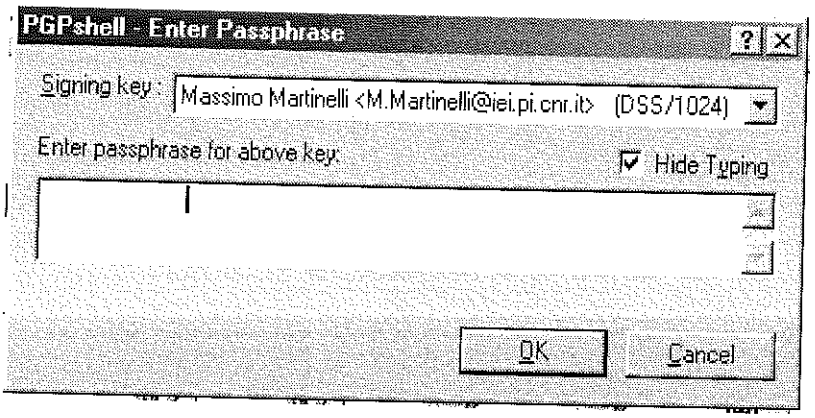


Encrypting a file for one person.

To encrypt and sign a file for 'Ovidio Salvetti' (no other in this case could decrypt the file), select it and with the right button of the mouse choose "PGP" and then "Encrypt & Sign"



You must enter your password



At this point the file is created (filename.extension.pgp).

Decrypt/Verify a file

1. Select the file or files that you want to decrypt and verify.
2. Right-click the file(s), point to PGP, and click Decrypt/Verify. The PGP Enter Passphrase dialog box appears asking you to enter your passphrase.
3. Enter your passphrase and then click OK.

   If the file is signed, a message appears indicating whether the signature is valid.

   If the text file is encrypted with Secure Viewer enabled, a warning message will appear.

4. You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.
5. Specify a filename and location for the decrypted version of the file. If you do not explicitly enter a name, the original name is used.
6. Click Save.

Checking a key's fingerprint

In the past, it was difficult to know if a key belonged to a particular individual unless that person physically handed the key to you on a floppy disk. Usually, exchanging keys in this way is not practical, especially for users who are located many miles far.
PGP includes a unique fingerprint associated with each key to verify that a key does without a doubt belong to the alleged owner.
The safest way to check a fingerprint is to call the person who read the fingerprint to you over the phone and compare it to the fingerprint on your copy of their public key.

To check a key's fingerprint, follow these steps:

1. Start PGPKeys
2. Highlight the public key for the fingerprint you want to verify.
3. Choose Properties from the Keys menu.
4. Use the series of words or characters displayed in the Fingerprint text box to compare with the original fingerprint.

By default, a biometric word list is displayed in the Fingerprint text box. However, you can select the Hexadecimal checkbox to view the fingerprint as a series of hexadecimal numbers.

Protecting your keys

In addition to make backup copies of your keys, you should take care about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and use your private key to crack your email or falsify your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the airwaves.