MacPGP 2.6.3 and its accompanying documentation and other support files are being distributed in a nested self extracting Stuffit archive. Since you are reading this file, you have already expanded the outermost archive. Besides this ReadMe you will find two other files:

MacPGP263_Folder.sea - this is the inner self extracting archive containing the actual program and support files

Macpgp263_Folder.sea.asc - this is a detached PGP signature on the preceding file

To verify that the archive you got has not been corrupted or tampered with, run a trusted copy of PGP (either a previous version of MacPGP or PGP for DOS/Unix). If you are verifying with a previous version of MacPGP use "Open/Decrypt" from the File Menu, then choose the file "Macpgp263_Folder.sea.asc" in the standard file dialog. Shortly thereafter MacPGP will ask you what file the signature applies to and you should then choose the file "MacPGP263_Folder.sea". If all goes well, PGP should display a message like this:

```
pgp 'PGP:Macpgp263_Folder.sea.asc'

File has signature.  Public key is required to check signature.

File 'PGP:Macpgp263_Folder.sea.$00' has signature, but with no text.
Text is assumed to be in file 'PGP:Macpgp263_Folder.sea'.
.
Good signature from user "Zbigniew Fiedorowicz <fiedorow@math.ohio-state.edu>".
Signature made 1996/06/27 16:39 GMT using 1022-bit key, key ID A20BD423
```

However this is only useful if you trust the key A20BD423. If you don't, then you should extract the key file keys.asc inside MacPGP263_Folder.sea. This file contains keys for people who were involved in development or distribution of recent versions of PGP. Add these keys to your pubring.pgp. Then choose "Check Signatures" from the Key menu. You will find two separate chains of trust linking the key A20BD423 to Philip Zimmermann's key C7A966DD

```
pub  1022/A20BD423 1992/09/30 Zbigniew Fiedorowicz <fiedorow@math.ohio-state.edu>
sig!     2416A859 1996/06/26  MacPGP Development

pub  1024/2416A859 1993/08/03 MacPGP Development
sig!     C7A966DD 1993/08/09  Philip R. Zimmermann <prz@acm.org>
```

and

```
pub  1022/A20BD423 1992/09/30 Zbigniew Fiedorowicz <fiedorow@math.mps.ohio-state.edu>
sig!     0500BF45 1995/01/11  Michael Paul Johnson <mpj@csn.org> mpj8

pub  1024/0500BF45 1994/06/27 Michael Paul Johnson <mpj@csn.org> mpj8
sig!     C7A966DD 1994/07/07  Philip R. Zimmermann <prz@acm.org>
```

Finally how do you verify that C7A966DD really belongs to Philip Zimmermann? Presumeably if you already have a trusted copy of PGP with which you are performing the verification, that key would have come together with it. Alternatively you might get hold of either of the following books on PGP:

> Protect Your Privacy - A Guide for PGP Users
> William Stallings
> Prentice-Hall, 1995
> ISBN 0-13-185596-4
>
> PGP: Pretty Good Privacy
> Simson Garfinkel
> O'Reilly Associates, Inc., 1995
> ISBN 1-56592-098-8

In the introduction to Stalling's book by Philip Zimmermann you will find the fingerprint for the key C7A966DD:

```
   9E 94 45 13 39 83 5F 70  7B E7 D8 ED C4 BE 5A A6
```

which you can compare against what you get when you choose "Fingerprint key" from the Key menu. Garfinkel's book lists the fingerprints of most of the keys in the file keys.asc on pages 261-262.

However the ultimate guarantee of trust in software like PGP is the free availability of the source code.

Note: If you perform the signature verification with a DOS/Unix version of PGP be sure you transfer the signature file "Macpgp263_Folder.sea.asc" in text mode,and the archive "MacPGP263_Folder.sea" in binary (not MacBinary) mode. If you are transfering the files to a DOS format diskette, PC Exchange (built into System 7.5) or similar extensions will automatically take care of this. (But you might want to rename the files beforehand to the DOS 8.3 format to avoid the artificial default DOS names which will otherwise be assigned.)