Quick-and-dirty distribution of PGP 2.6.3i for NEXTSTEP

Gerben Wierda
R&A

0. Introduction

This is a quick-and-dirty distribution of PGP for NEXTSTEP. The package can install the binaries and other stuff for you. This file contains minimal instructions to get up and running. This distribution is meant as an easy companion for EnhanceMail, which nowadays contains a PGP interface.

This is a quick-and-dirty installation. It has not been tested (the pgp software inside it has been tested on m68k and i486, but the package has not, but it is fairly simple).

1. Files

The following files can be found in this distribution:

```
PGP-2.6.3i.NIHS.README.rtf      This file
```

```
PGP-2.6.3i.NIHS.b.pkg.tar      The installation package in a tar file (563200 bytes)
PGP-2.6.3i.NIHS.b.pkg.tar.asc  The transport armor file of the tar file (286 bytes)
```

1.1 The installation package

The package `PGP-2.6.3i.NIHS.b.pkg` has been compacted with gzip_package. This means that the compressed .tar.Z file inside the package has been replaced by a gzipped version and that there is a pre-install script. Don't worry about this script (read it), it is just for recreating the normal .tar.Z file so that Installer.app knows what to do. It also means that if you copy the package somewhere you will encounter a symbolic link. When copying that link, make sure to create a new link.

2. Installation

2.1 installing the PGP system

Untar the tar file somewhere or open it with 'Opener.app'. This produces the file `PGP-2.6.3i.NIHS.b.pkg`

As root: Start Installer.app and open the file PGP-2.6.3i.NIHS.b.pkg. Install.

Default location is /usr/local, this implies that the files/directories

```
/usr/local/bin/pgp
/usr/local/lib/pgp
/usr/local/man/man1/pgp.1
```

will be created.

2.2 Creating your PGP directory and keyrings

Log in as yourself. Start up a shell (e.g. Terminal.app). In the shell type

```
pgp
```

you should see:

```
Pretty Good Privacy(tm) 2.6.3ia - Public-key encryption for the masses.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
International version - not for use in the USA. Does not use RSAREF.
Current time: 1996/10/24 14:28 GMT

For details on licensing and distribution, see the PGP User's Guide.
For other cryptography products and custom development services, contact:
Philip Zimmermann, 3021 11th St, Boulder CO 80304 USA, phone +1 303 541-0140
```

```
For a usage summary, type:  pgp -h
```

If you don't see the above, but instead you see
```
pgp: Command not found.
```

/usr/local/bin (or wherever you installed PGP) is not part of your path. Make it so, or use the full path, e.g.
```
    /usr/local/bin/pgp
```

Now, create a directory for your keyrings:

```
    mkdir ~/.pgp ; chmod 600 ~/.pgp
```

Now, create your first key. Type

```
    pgp -kg
```

and follow the instructions.

3. Armor

The armor of the tar file is:

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

iQCVAwUAMm+DW8VJHpXdYPtlAQFuCQP/QE+aCysRiik4yv2h18aF+TMDEPEHl6pW
bW0pq8uy1Rdbn4L1zpKwX31V8P+fhQnk4Aj1A/ByRN5qYxF89jB3snHT1vD+dtxY
yQoB3SM37b+fVwR3CuUt8GobIpUAtmOpJe2lKfiJaEW3FVtchKFhNzr7IGlWhGVN
ft2ZCc8AP4I=
=OzhJ
-----END PGP MESSAGE-----
```

You can check if you have received the right tar file by running

```
pgp PGP-2.6.3i.NIHS.b.pkg.tar.asc PGP-2.6.3i.NIHS.b.pkg.tar
```

And the result should be like:

```
Pretty Good Privacy(tm) 2.6.3ia - Public-key encryption for the masses.
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04
International version - not for use in the USA. Does not use RSAREF.
Current time: 1996/10/24 14:20 GMT

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

File 'PGP-2.6.3i.$00' has signature, but with no text.
Text is assumed to be in file 'PGP-2.6.3i.NIHS.b.pkg.tar'.
.
Good signature from user "G.C.Th.Wierda@AWT.nl".
Signature made 1996/10/24 14:08 GMT using 1024-bit key, key ID DD60FB65

Signature and text are separate.  No output file produced.
```