CEDPGP

Janusz A. <alex@vm.cc.uni.torun.pl>

COLLABORATORS

	TITLE : CEDPGP		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Janusz A. <alex@vm.cc.uni.torun.pl>	July 22, 2024	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

CEDPGP

1.1 CED <-> PGP Interface documentation

```
      CED <-> PGP Interface

     © 1994 Janusz A. Urbanowicz <alex@vm.cc.uni.torun.pl>

       AmigaGuide® Manual

  Contents:

     Legal Issues

    @{ " Copyrights      " link cpr }
    @{ " Distribution    " link dist }

     Product Info

    @{ " Description     " link selfinfo } What it is ?
    @{ " About PGP       " link PGP } What is PGP
    @{ " Requirements    " link config } What you need to use it
    @{ " History         " link history } Previous versions
    @{ " Miscellanea     " link author } Author info and acknowledgements

     User Manual

    Installation

    @{ " Scripts         " link scripts } General remarks
        @{ " SignPGP     " link sign } Sign function
        @{ " EncryptPGP  " link crypt } Encrypt function
        @{ " EncipherPGP " link cipher } Conventional encryption function
        @{ " DecryptPGP  " link decrypt } decrypts all ASCII @{ " PGP " link PGP } ↩
            packets

    @{ " Troubleshooting " link troubles } Solutions to most possible problems
```

1.2 Copyrights

1.3 Distribution terms

@{ " Distribution " link GPL/GPL 60 } of The Interface is managed by @{ " GNU General Public License "link GPL/GPL }.

You may copy and modify The Interface as you wish (under GNU GPL
conditions), but it would be very nice of you to make me know about changes
you make to The Interface, because I'd want to incorporate these
changes in next offcial release of The Interface.

The official release of The Interface is signed using PGP with
my @{ " public key " link key }. You may check validity of the signature using @{ " PGP " link PGP }.

I made The Interface freely distributable because I wrote it for the people.
You do not have to send me anything material like cash, or postcard,
or something else. You don't have to send me anything at all (even e-mail),
but its nice of you to make me know you use effect of my work.

1.4 What is it

This software is a set of four scripts that integrate PGP software
package in one with your ASDG Cygnus Editor program. This software uses
Amiga's unique ARexx inter-program interface to make all major PGP
functions avaliable within CED. The supported PGP functions are: Encrypt,
Conventional Encryption, Decrypt and Sign.

@{ " PGP " link PGP } itself is written to allow people use public key cryptography
easily, and it does so. But to fully use its power, it is needed to
integrate @{ " PGP " link PGP } with other software.

Here comes this software - when you use it you may forget how @{ " PGP " link PGP } works.
You install @{ " PGP " link PGP }, generate you key and install those scripts. Then you
may forget how @{ " PGP " link PGP } works, those scripts will do all for you.

To simplify some things I will call this package (CED <-> PGP Interface)
The Interface in this documentation.

I tried to make The Interface as foolproof and bug-free as possible,
without losing security. I don’t know if I succeeded. If you have any
remarks about The Interface, @{ " e-mail " link author } me.

1.5 What is PGP

This was written by Philip R. Zimmermann. This text is quoted from PGP
documentation.

Quick Overview
****

Pretty Good(tm) Privacy (PGP), from Phil’s Pretty Good Software, is a high
security cryptographic software application for MSDOS, Unix, VAX/VMS, and
other computers. PGP allows people to exchange files or messages with
privacy, authentication, and convenience. Privacy means that only those
intended to receive a message can read it. Authentication means that
messages that appear to be from a particular person can only have
originated from that person. Convenience means that privacy and
authentication are provided without the hassles of managing keys
associated with conventional cryptographic software. No secure channels
are needed to exchange keys between users, which makes PGP much easier to
use. This is because PGP is based on a powerful new technology called
"public key" cryptography.

PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key
cryptosystem with the speed of conventional cryptography, message digests
for digital signatures, data compression before encryption, good ergonomic
design, and sophisticated key management. And PGP performs the public-key
functions faster than most other software implementations. PGP is public
key cryptography for the masses.

If you don’t have PGP, The Interface won’t be useful to you,
see @{ " requirements " link config }.

1.6 Hardware and software requirements

To use The Interface you have to have:

- any Amiga - compatible computer
- the @{ " PGP " link PGP } package
- ASDG Cygnus Editor, and please, buy original
- ARexx

ARexx is a part of system software since 2.04. If you have system 1.3 or lower, you must purchase ARexx separately. It's a commercial product.

The Interface needs the PIPE: device to be mounted. It will not work without it.

1.7 The most possible troubles with The Interface

The most possible problem with The Interface is that it won't detect your PGP binary version number. There are two solution to this:

- make PGP binary avaliable in your system in way that will allow The Interface to @{ " check its version number " link vercheck } . This may be done via copying the file somewhere else or making a link in filesystem (I use this method).
- using CED or other text editor (but you have CED, isn't it ?), you may cut all below 'checkf:' label in all scripts and put there 'Return 0' if you using other PGP than 2.3a.[3-5], or 'Return 1' if you are using this version.

Sorry for the mess, but I had to do it to increase security.

During writing of The Interface I once encountered problem with passing environmental variables to ARexx using PIPE: device. This bug was unrepeatable and I am not sure if it was my fault.

IF YOU HAVE PROBLEMS WITH THIS PLEASE @{ " LET ME KNOW ! " link author }

1.8 How The Interface checks PGP version number

Because of some features that are avaliable in PGP 2.3a.[3-5] I had to make The Interface check which version of PGP user has installed. This is based on two assumptions I made. If

- PGP binary is in AmigaDOS path, or
- PGP binary is in $PGPPATH,

then The Interface will use special PGPAmiga features (or won't try to use any of them if they are not avaliable in version of PGP you use).

1.9 Author info & thanx

If you want to contact me, I am reachable via e-mail as:

- alex@vm.cc.uni.torun.pl
  flatline@mat.uni.torun.pl In InterNet

- ALEX AT PLTUMK11 In BitNET/EARN

I am also subscribed to PGPAmiga users mailing list, at address
PGPAmiga@peti.GUN.de . This address is good also if you want to contact
other crypto-freaks or Peter Simons who ported PGP to Amiga.

If you want more info on me, I have WWW page which contain the most
important informations. The URL is:

http://vm.cc.uni.torun.pl:70/Web/Alex/alex.html

I want to thank:

- Peter Simons, who ported PGP GS Draw File: Copyright Golden Software Inc. ↩
  1991-1992RSØfïê| ØâPtFtö(w
??2ÿ<~????2_"??¯?????Li??Ò)w"?t,w"?????????2?3?4?54N??X Axis ↩
  1??????????????????????????????????°??????????????????@@?????@@?????@¿@ ↩
  ?? ??? ???k ↩
  ?????????????i@??????Y@??????????" link PGP } to Amiga and made it superior
  to other platforms versions.

- Joerg Plate and Rick Younie whose ideas were significant
  improvement to The Interface.

- people who created the Amiga. It doesn't matter what others say.
  It is only user-friendly machine I like. And for me
  it always be a dream machine.

- Amiga, for being the best personal computer ever !

And last but not least, here is my PGP @{ " public key " link key }.

1.10 Author's PGP public key

To add this key to your public keyring, make sure that @{ " PGP " link PGP } is
in your path and type 'PGP -ka CEDPGP.guide' (in shell of couse).

1.11 Remarks

There are four ARexx scripts in The Interface. Each of them calls
only one major @{ " PGP " link PGP } functions. This is because @{ " PGP " link ↩
PGP } behaves
differently when using different functions:

@{ " SignPGP " link sign } signs file using @{ " PGP " link PGP } Sign functions
@{ " EncryptPGP " link crypt } encrypts file with given userid’s public key
@{ " EncipherPGP " link cipher } encrypts file with Conventional encryption option
@{ " DecryptPGP " link decrypt } decrypts all information (non-key) @{ " PGP " link PGP } packets

Scripts are standalone ARexx programs, they do not call each other, but
they have some code common to all. This code detects @{ " PGP " link PGP } version number,
and asks for passphrase when its necessary. This is made because @{ " PGP " link PGP }
official port made by Peter Simons has builtin passphrase requester. It was
impossible to conceal typed passphrase using Cygnus Editor functions, so
The Interface uses @{ " PGP " link PGP } builtin feature when its avaliable.

If your @{ " PGP " link PGP } @{ " version " link vercheck } is 2.3a[3-5], but there is no passphrase requester
when @{ " PGP " link PGP } is used with The Interface, see @{ " troubleshooting " link troubles }.

If you want to use other key than default for signing, you may do this via
setting PGPUSER environmental variable. You set it to value that you would
use with ’-u’ option.

1.12 About SignPGP.ced

This script was first of all, and this is "mother" of all other scripts.
Especially Encrypt and Encipher was based on it.

When run, may ask for your passphrase if necessary then asks if you want to
set transparency option. If this option is set, @{ " PGP " link PGP } signature is added
at the bottom. If not, signature is added, and whole text is ASCII armored.
If there is no block marked in the text for signing, user is asked if he
wants to sign whole file.

This script utilizes @{ " PGPUSER " link scripts 20 } environmental variable.

History:

Version 1.0 - First private version

Version 1.1 - Added interpretation of PGPUSER variable

Version 1.2 - Added choice between standard and clearsigning

Version 1.2.1 - small cosmetical changes

Version 1.3 - checks if it is possible to use PGP’s internal
passphrase requester (PGP 2.3a.[3-5] only)

Version 1.4 - added ’Sign whole file ?’ option

Version 1.5 - support for PGP26_IMPERSONATE option added

Version 1.6 - checking PGP version number improved. Now PGP
has only to be in ADOS path, not in $PGPPATH

Version 1.6.1 - fixed misfeature - the signed text was lost if
PGP was in filter mode and used gave wrong password
Also undo used intead of inserting cut text when user
supplied wrong passphrase

Version 1.6.2 - small changes to code, plus detection of 2.3a.5

Version 1.6.3 - bugfix. This version was first avaliable via
WWW.

Version 1.7 - this version is final for now. Added are:

- Whole PGP output is visible in CON: window on
  CED’s screen. Thanx for that goes to Rick Younie
  <rick@freenet.vancouver.bc.ca>.
- Script recognizes if there is more than one CEDs
  running and works with right one. Thanx for that goes to
  Joerg Plate <Joerg.Plate@arbi.informatik.uni-oldenburg.de>.
- version 2.6ui is probably detected (I had no opportunity to
  test.. :-( )

1.13 About EncryptPGP.ced

This is IMHO main script of The Interface. It utilizes main @{ " PGP " link PGP } feature
- public key cryptography. User is asked about userid of public key,
the text will be encrypted with. Also it is possible to sign text using
user’s private key. In this case user is asked for his passphrase.
If there is no block marked when this script is called, user may choose
to encrypt whole file.

This script utilizes @{ " PGPUSER " link scripts 20 } environmental variable.

History:

Version 1.0 - First posted to PGPAmiga Mailing List. Simple.

Version 1.2 - Added ’Encrypt whole file ?’ question and makes
use of PGP 2.3a.[3-4] internal passphrase requester.
Major rewrite, based on @{ " SignPGP.ced 1.6 " link sign 28}.

Version 1.2.1 - now properly detects if PGP 2.3a.[3-4] quit
on wrong passphrase.

Version 1.2.2 - using CED undo function instead inserting cut
text when user had given wrong passphrase.

Version 1.2.3 - minor, almost meaningless fix, plus patchlevel
5 version detection added

Version 1.3 - 2.6ui version detection added, plus numerous features

```
    descibed at @{ " SignPGP.ced version 1.7 " link sign 49 } .
```

1.14 About EncipherPGP.ced

```
This script allows you to use Conventional Encryption optio
```