1 What is gpgmailencrypt

gpgmailencrypt can encrypt e-mails.

It supports

* PGP/Inline

* PGP/Mime

* SMime

It can be used normally as a script doing everything on command line or in daemon mode, where gpgmailencrypt acts as an encrypting smtp server.

It takes emails and if a encryption key exists for this user it will return the e-mail encrypted to another e-mail server.

The encryption method can be selected per user.

1.1 Prerequisites

The following software needs to installed

- python 2.x
- gnupg (I recommend version 2)
- openssl

1.2 PGP versus SMIME

todo

2 Installation

2.1 General

1. Copy the file „gpgmailencrypt.py“ into the directory /usr/local/bin and make the file executable via

   ```
   sudo chmod 755 /usr/local/bin/gpgmailencrypt.py
   ```

2. Create a default configuration file via

   ```
   gpgmailencrypt.py -x > ~/gpgmailencrypt.conf
   ```

3. Copy the configuration file into the directory /etc

```
sudo cp ~/gpgmailencrypt.conf /etc
```

2.2 Daemon

1. Copy the file gpgmailencrypt.init into the directory /etc/init.d via

```
sudo cp gpgmailencrypt.init /etc/init.d/gpgmailencrypt
```

2. Create a user (gpg-mailencrypt) under which the daemon should run

```
sudo adduser gpg-mailencrypt
```

3. You can set the user in the file /etc/default/gpgmailencrypt. It should contain

```
USER="gpg-mailencrypt"
DIR=”/usr/local/bin”
```

3 Configuration /etc/gpgmailencrypt.conf

3.1 General

```
[default]
prefered_encryption = gpginline          ; valid values are
'gpginline','gpgmime' or 'smime'
add_header = no                          ; adds a X-GPGMailencrypt header to
the mail
domains =                                ; comma separated list of domain
names, that should be encrypted, empty is all
spamsubject =***SPAM                ; Spam recognition string, spam will not be
encrypted
output=mail                              ; valid values are 'mail'or 'stdout'
locale=en                           ; DE|EN|ES|FR'

[logging]
log=none                            ; valid values are 'none', 'syslog', 'file'
or 'stderr'
file = /tmp/gpgmailencrypt.log
debug = no

[mailserver]
host = 127.0.0.1                    ;smtp host
port = 25                           ;smtp port

[usermap]
;user_nokey@domain.com = user_key@otherdomain.com

[encryptionmap]
user@domain.com = PGPMIME           ;PGPMIME|PGPINLINE|SMIME|NONE
```

3.2 PGP specific configuration

```
[gpg]
keyhome = /var/lib/gpgmailencrypt/.gnupg       ; home directory of public
gpgkeyring
gpgcommand = /usr/bin/gpg2
allowgpgcomment = yes                     ; allow a comment string in the GPG
file
```

3.3 SMIME specific configuration

```
[smime]
keyhome = ~/.smime                        ;home directory of S/MIME public key
files
opensslcommand = /usr/bin/openssl
defaultcipher = DES3                      ;DES3|AES128|AES192|AES256
extractkey= no                            ;automatically scan emails and extract
smime public keys to 'keyextractdir'
keyextractdir=~/.smime/extract

[smimeuser]
smime.user@domain.com = user.pem[,cipher] ;public S/MIME key file [,used cipher,
see defaultcipher]
```

3.4 Daemon specific configuration

```
[daemon]
host = 127.0.0.1                    ;smtp host
port = 10025                        ;smtp port
```

4 Key Managment

The following commands have to be used as the user, that is running gpgmailencrypt. Remember that in daemon mode this user is 'gpg-mailencrypt'. So for daemon mode you first have to change the user

```
sudo su - gpg-mailencrypt
```

4.1 PGP

Add a PGP key to the public key ring

```
gpg --import publickey.gpg
```

4.2 SMIME

Smime keys are stored in the directory ~/.smime per default. You have to create it if it does not exist. Each key is stored in a single file in pem-format.

Usually you get the smime.key file in a different format. To convert it use

```
openssl pkcs7 -print_certs -inform DER -in smime.p7s -out smime.pem
```

Let's say you get the smime.p7s from agentj@mib.

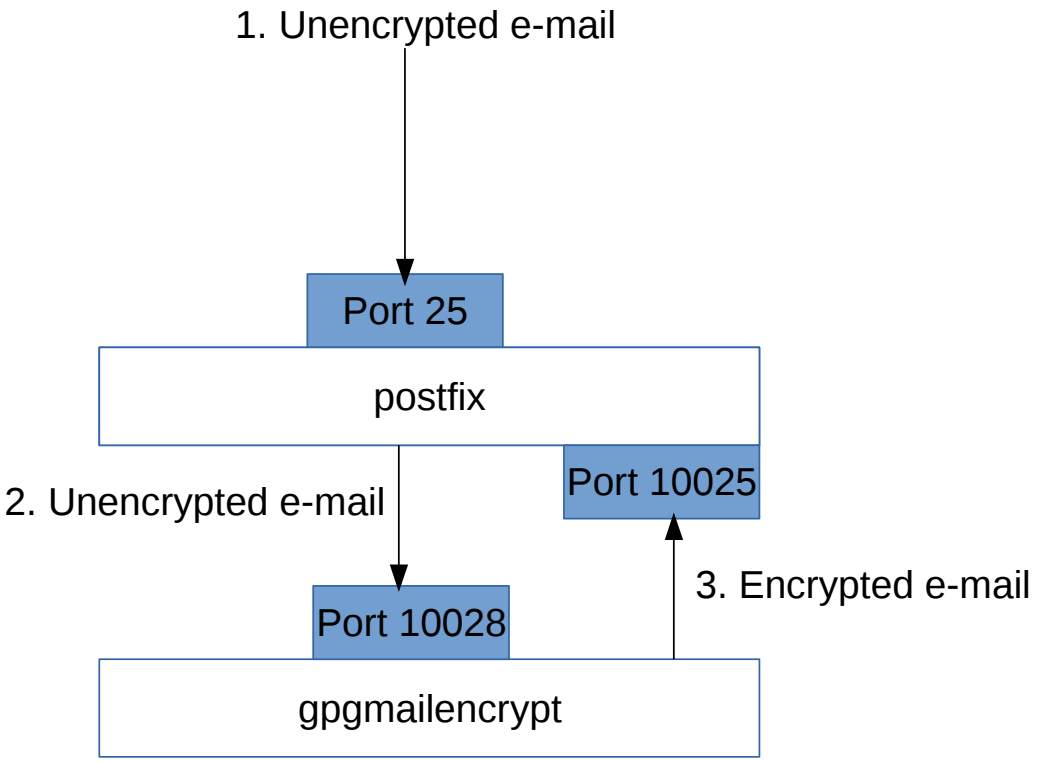
Instead of 'smime.pem" you should use a unique name for the file and copy it in ~/.smime/

```
cp smime.pem ~/.smime/agentj@mib.pem
```

For this user you need also an entry in /etc/gpgmailencrypt.conf

```
[smimeuser]
agentj@mib = agentj@mib.pem
```

5 Integrating gpgmailencrypt in postfix



Install and configure gpgmailencrypt as daemon.

/etc/gpgmailencrypt.conf

```
[mailserver]
host = 127.0.0.1
port = 10025
[daemon]
host = 127.0.0.1
port = 10028
```

/etc/postfix/main.cf

```
content_filter=gpgmailencrypt:[127.0.0.1]:10028
```

/etc/postfix/master.cf

```
localhost:10025 inet n - n - -  smtpd
        -o content_filter=
        -o mynetworks=127.0.0.0/8
        -o receive_override_options=no_unknown_recipient_checks
        -o smtpd_recipient_restrictions=permit_mynetworks,reject_unauth_destination
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8

gpgmailencrypt unix - - n - 2 smtp
        -o smtp_data_done_timeout=1800
```