# 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

# 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
authenticate = False                     ;user must authenticate
smtpcredential =/etc/gpgmailencrypt.cfg  ;file format 'user=password'

[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
smtps = False                       ;use smtps encryption
sslkeyfile = '/etc/gpgsmtp.key'           ;the x509 certificate key file
sslcertfile = '/etc/gpgsmtp.crt'          ;the x509 certificate cert file
authenticate = False                      ;users must authenticate
smtppasswords = '/etc/gpgmailencrypt.pw'  ;use smtps encryption
```

The gpgmailencrypt.pw has the following format:

```
user1=password1
user2=password2
```

Don't forget to make the file readable only for the gpgmailencrypt user!

The x509 certificate files can be created see:

```
https://www.e-rave.nl/create-a-self-signed-ssl-key-for-postfi
```

# 4 Key Management

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.

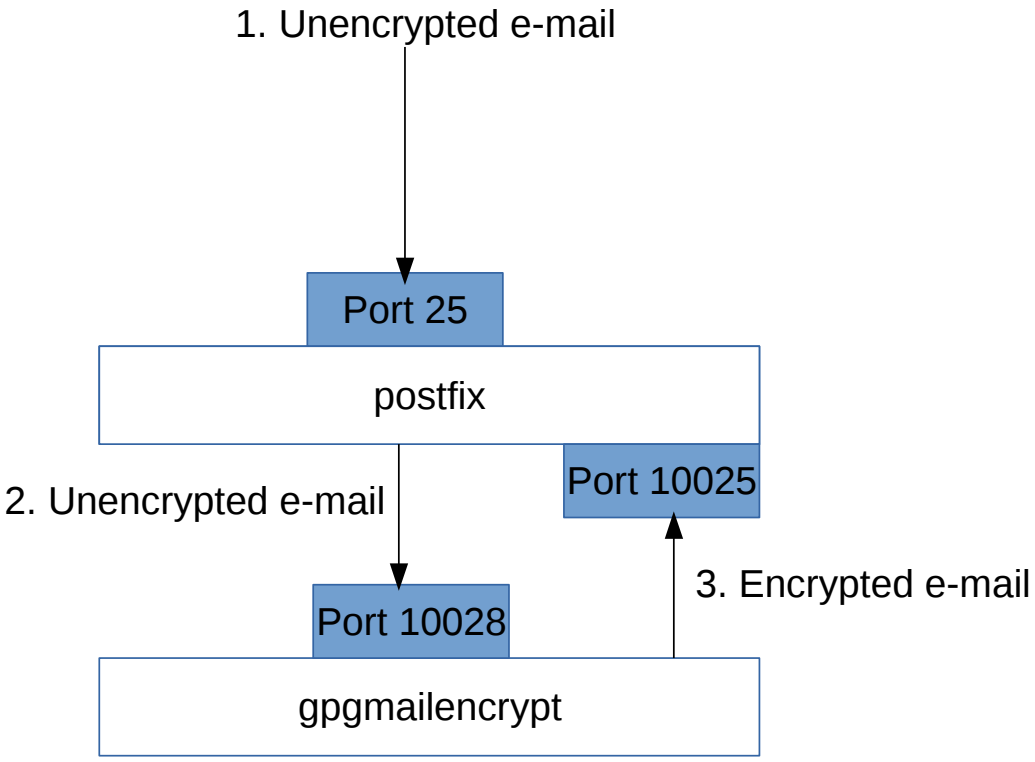
Instead of 'smime.pem" you should use a unique name for the file and copy it in ~/.smime/

```
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
```

## 5.1 Using authentication

For using the authentication add the following to gpgmailencrypt section in master.cf

```
        -o smtp_sasl_auth_enable=yes
        -o smtp_sasl_password_maps=hash:/etc/postfix/gpgmailencrypt_passwd
```

With /etc/postfix/gpgmailencrypt_passwd having the following structure

```
localhost user:password
```

Then use the following commands

```
sudo chmod 640 /etc/postfix/gpgmailencrypt_passwd
sudo postmap /etc/postfix/gpgmailencrypt_passwd
```

## 5.2 Using smtps

To use the gpgmailencrypt smtps feature  with postfix 2.x you need to install stunnel (in Ubuntu the package is called stunnel4)

Create the file /etc/stunnel/gpgmailencrypt.conf

```
[gpgmailencrypt-smtps]
    accept = 10000
    client = yes
    connect = localhost:10028
```

And change /etc/default/stunnel4

```
ENABLED=1
```

Then start stunnel with

```
/etc/init.d/stunnel4 start
```

/etc/postfix/main.cf should be changed to

```
content_filter=gpgmailencrypt:[127.0.0.1]:10000
```