

[Log In](#)

[Revisions](#)

[PDF](#)

[Home](#)

[Search](#)

[Contact](#)

[News](#)

[Admin](#)

You are here: [start](#) / [networking](#) / [dovecot](#) / [encrypting_mail_folders](#)

-Table of Contents

- [About](#)
- [Requirements](#)
- [Generating Encryption Keys](#)
- [Configuring Dovecot](#)
- [Testing Encryption](#)
- [Encrypting old E-Mails](#)

About

Regrettably, Dovecot (and many other servers implementing mail protocols such as IMAP and POP) does not encrypt received mails by default when placing them into the user folder or into the system-wide user mailbox. It is very easy for a system administrator, sub-administrator or even plain users to read emails in case mailbox folders do not have the correct permissions set. In large setups where the mail server allows users to log-in, it becomes rather trivial to read a different user's E-Mail.

Dovecot offers a mail encryption plugin that will encrypt mails as they arrive and place them in the receiving user's mailbox. This is done by dovecot with administrator-generated keys such that recovery is possible for an administrator but at least users with no access to the dovecot configuration have no chance of recovering the mail plaintext even with broken FSH permissions.

Requirements

- a Dovecot install over or equal to version 2.2.27.

Generating Encryption Keys

Dovecot can be configured with per-folder keys or with global keys but [the documentation](#) implies that per-folder keys are not ready for production so global keys will be used in this tutorial instead.

Create the folder `/etc/dovecot/mailcrypt` to hold the generated keys:

```
mkdir -p /etc/dovecot/mailcrypt
```

Next, issue:

```
openssl ecparam -list_curves
```

to list elliptic curve parameters for generating keys.

You can pick any you like or trust most, say `brainpoolP512t1`, and then issue:

```
openssl ecparam -name prime256v1 -genkey | openssl pkey -out  
/etc/dovecot/mailcrypt/ecprivkey.pem
```

to generate a private key.

Next, issue:

```
openssl pkey -in /etc/dovecot/mailcrypt/ecprivkey.pem -pubout -out  
/etc/dovecot/mailcrypt/ecpubkey.pem
```

to generate the public key.

Now both `ecprivkey.pem` and `ecpubkey.pem` should be in `/etc/dovecot/mailcrypt`.

Configuring Dovecot

With both private and public keys, create a file `/etc/dovecot/conf.d/10-mailcrypt.conf` with the following contents:

```
mail_plugins = $mail_plugins mailcrypt  
  
plugin {  
    #fts_index_fs = crypt:set_prefix=fscrypt_index:posix:set_prefix=/tmp/fts  
    mailcrypt_global_private_key = PRIVATE_KEY  
    mailcrypt_global_public_key = PUBLIC_KEY  
    mailcrypt_save_version = 2  
}
```

The `PRIVATE_KEY` and `PUBLIC_KEY` parameters have to be replaced with the contents of the files generated in `/etc/dovecot/mailcrypt/` - unfortunately, due to a bug, Dovecot cannot yet read the

keys from the files such that they will have to be inlined. For instance, after replacing the variables, the `/etc/dovecot/conf.d/10-mailcrypt.conf` file will look similar to:

```
mail_plugins = $mail_plugins mail_crypt

plugin {
  #fts_index_fs = crypt:set_prefix=fscrypt_index:posix:set_prefix=/tmp/fts
  mail_crypt_global_private_key = P01grDe40QMPss76IYStV9SBlrGH9JnwZgnbn...
  mail_crypt_global_public_key = EBgiuARr369YLt/hYP0h8olBYb4PIwBGV09Jg...
  mail_crypt_save_version = 2
}
```

Optionally, if [E-mail full-text search](#) has been enabled, the `fts_index_fs` configuration key can be enabled by removing the hash sign (#) in front.

With the configuration in place, issue:

```
/etc/init.d/dovecot restart
```

to restart Dovecot.

Testing Encryption

Dovecot will now encrypt incoming mails so an easy way to check that the encryption works is to send an E-mail from a different account and then browse the user's mailbox folder. All new emails should be in binary format and the contents should be encrypted.

Encrypting old E-Mails

Unfortunately, old E-mails will not be encrypted and to encrypt them it is necessary to export the mailbox using `doveadm / dsync` and then migrate to the newly encrypted mailbox.

As the user for which to encrypt mails, issue:

```
doveadm -vf sync sdbox:~/sdbox.crypt
```

which will export the mailbox at `~/sdbox` to `~/sdbox.crypt`. The `~/sdbox.crypt` folder will have the same contents as `~/sdbox` but with the E-mails encrypted.

The final step is to move the old `~/sdbox` out of the way and rename `~/sdbox.crypt` to `~/sdbox`.

networking/dovecot/encrypting_mail_folders.txt · Last modified: 2022/04/19 08:27 by 127.0.0.1

You are here: [start](#) / [networking](#) / [dovecot](#) / [encrypting_mail_folders](#)

[Log In](#)

[Revisions](#)

[PDF](#)

[Home](#)

Search

Contact

News

Admin

For the contact, copyright, license, warranty and privacy terms for the usage of this website please see the [contact](#), [license](#), [privacy](#), [copyright](#).