

Mailit 11 supports the PGP encryption standard.

PGP (Pretty Good Privacy) is a proven method of protecting email communication with end-to-end encryption which prevents emails from being read by any third parties, including your email provider.

PGP works with a key pair: a public key and private key, but it is also possible to encrypt messages without keys using only a passphrase. The public key can be distributed to anyone who wants to send you a message and is used to encrypt a message that can only be decrypted by you. In order to create a public and private key, you can use the pgp console utility. If you do not have the pgp utility, the easiest way is to use online services for creating keys, for example:

<https://pgptool.org/>
<https://pgpkeygen.com/>
<https://onlinepgp.com/>

Note. When creating keys, you will need to indicate your name and your email. For example:

Your Name: Test Box

Your email: testbox@dacons.net

When creating an encrypted message, the “To” recipient field must contain the same name and email, example: “Test Box <testbox@dacons.net>”. The same goes for the “From” field.

At the output of online services or the pgp utility, you should have two .asc files, which are a public and a private key.

The sender's private key is used to send a signed message. The recipient can verify the message signature using the sender's public key.

The recipient's public key is used to create an encrypted message. The recipient can decrypt the message using his private key.

When creating a signed and encrypted message, the message is first signed and then encrypted. The recipient must first decrypt the message and then verify the digital signature.

Start with example files.

The Mailit 11 plugin comes with two demos: Simple Sending.fmp12, Simple Receiving IMAP.fmp12.

If you want to test the example files yourself and you don't have a friend/recipient who has PGP configured, then you'll need two mailboxes. Use one mailbox in the file “Simple Sending.fmp12” to send a message. Use the second mailbox in the “Simple Receiving IMAP.fmp12” file to receive messages sent from the first mailbox. For two mailboxes, you need to create a public key/private key pair.

After you do this, you can start setting up the examples.

Configuring message sending in the Simple Sending.fmp12 file

Below is an instruction that uses a public/private key pair. If you want to try encryption using only a passphrase, then skip the steps that require setting up keys.

Open the file “Simple Sending.fmp12” and click on the icon  in the upper right corner, this way you will go to the account management layout.



On the account management layout, click the plus “+” icon, which is located at the top left, in order to create a new account.

Next, fill in the required fields to connect to the SMTP server. Then click the “Test Connection from FM” button to test the connection.

The screenshot shows the 'Accounts' management interface. On the left, a list of accounts includes 'testbox@dacons.net' and 'beta@dacons.net'. A red box labeled '1' highlights the plus icon at the top of this list. The main area is titled 'General Account Settings' and contains several input fields. A red box labeled '2' encompasses the 'Name' (Test Box), 'Email Address' (testbox@dacons.net), 'SMTP Server' (smtp.1und1.de), 'SMTP Server Port' (587), 'SSL/TLS' (On), 'SMTP Server Timeout' (30), 'SMTP Authentication only' section (including 'Pref. SMTP Auth.' set to LOGIN, 'SMTP User Name' testbox@dacons.net, 'SMTP Password' masked with dots, and 'SMTP Domain' with a hint), and the 'Test Connection from FM' button. A red box labeled '3' highlights the 'Test Connection from FM' button. At the bottom, the 'Date Settings' section includes 'Add Time Stamp' (On) and 'Time Zone' (+0300).

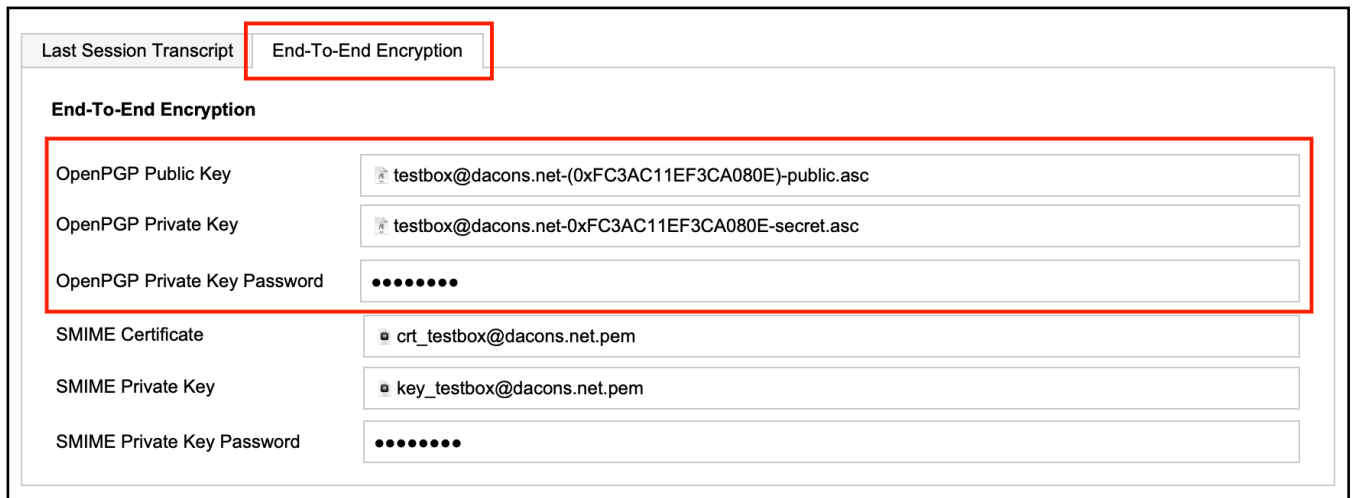
Field	Value
Name	Test Box
Email Address	testbox@dacons.net
SMTP Server	smtp.1und1.de
SMTP Server Port	587
SSL/TLS	On
SMTP Server Timeout	30
Pref. SMTP Auth.	LOGIN
SMTP User Name	testbox@dacons.net
SMTP Password	••••••••
SMTP Domain	Hint: NT Domain (only for 'NTLM' auth. type)

Buttons: Test Connection from FM, Test Connection from FMS

Date Settings: Add Time Stamp (On), Time Zone (+0300)

Note. Some servers allow you to establish a connection with incorrect login/password data. When you click the “Test Connection from FM” button, the plugin connects to the server but does not send a test message. Therefore, this is basically checking the connection to the server to make sure that the firewall or antivirus is not blocking the connection. But if an incorrect login/password was specified and the server ignored it, then you will find out that the login/password is incorrect at the time the message is sent.

Next, go to the “End-To-End Encryption” tab and drag your public key file into the “OpenPGP Public Key” field, and your private key file into the “OpenPGP Private Key” field, also into the “OpenPGP Private Key Password” specify the password for the private key.



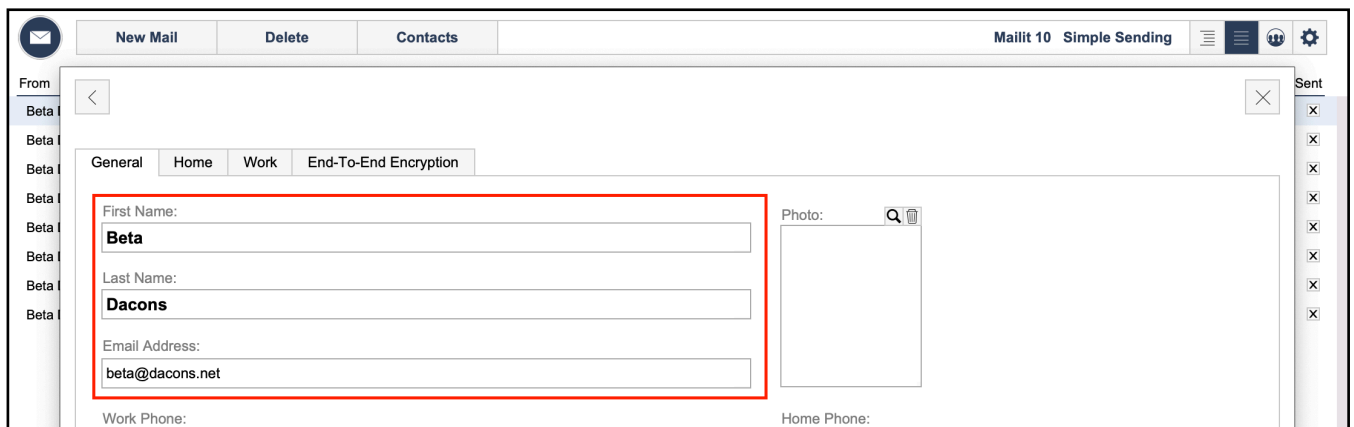
Account setup is complete, click the cross icon in the upper right corner.



Now you need to create a recipient entry in your contact book. Click the “Contacts” button in the top menu. In the window that opens, click the “+” icon to create a new contact.



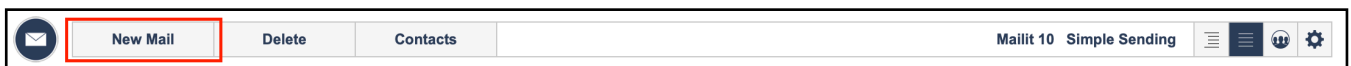
For a new contact, enter your First and Last Name and email address in the appropriate fields.



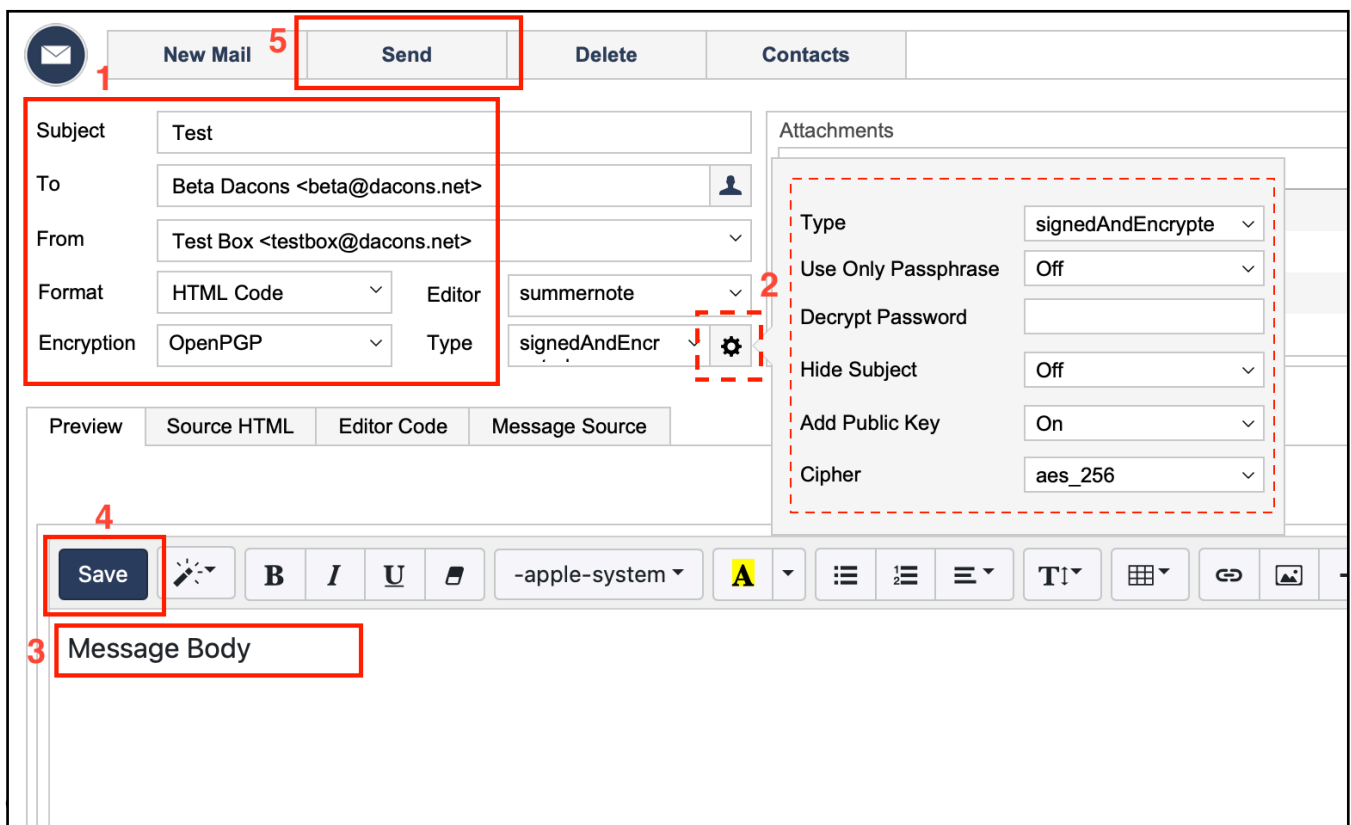
Go to the "End-To-End Encryption" tab and drag the recipient's public key file into the "OpenPGP Public Key" field.



Now that you have set up an SMTP account and created one recipient, you can create a message. In the top menu, click the "New Mail" button to create a new message.



In the message subject field, enter the subject of the message.
In the "To" recipient field, click the button at the end of the field to select a recipient from the address book. In your address book, click on the contact you created.
In the "From" field, select your account.
In the "Encryption" field, select "OpenPGP".
In the "Type" field, select the type of operation, signed, encrypted or signed and encrypted of the message. By clicking on the gear at the end of the Type field you can specify additional settings.
Next, write some text in the body of the message and click the "Save" button.



If you use the example file without a public/private key pair, only with a passphrase. Then in the “OpenPGP” settings, select “encrypted” in the “Type” field, click on the gear at the end of the field to display additional options. In the “Use Only Passphrase” field, select “On”. In the “Decrypt Password” field, enter the password phrase that the recipient will need to use to decrypt the message.

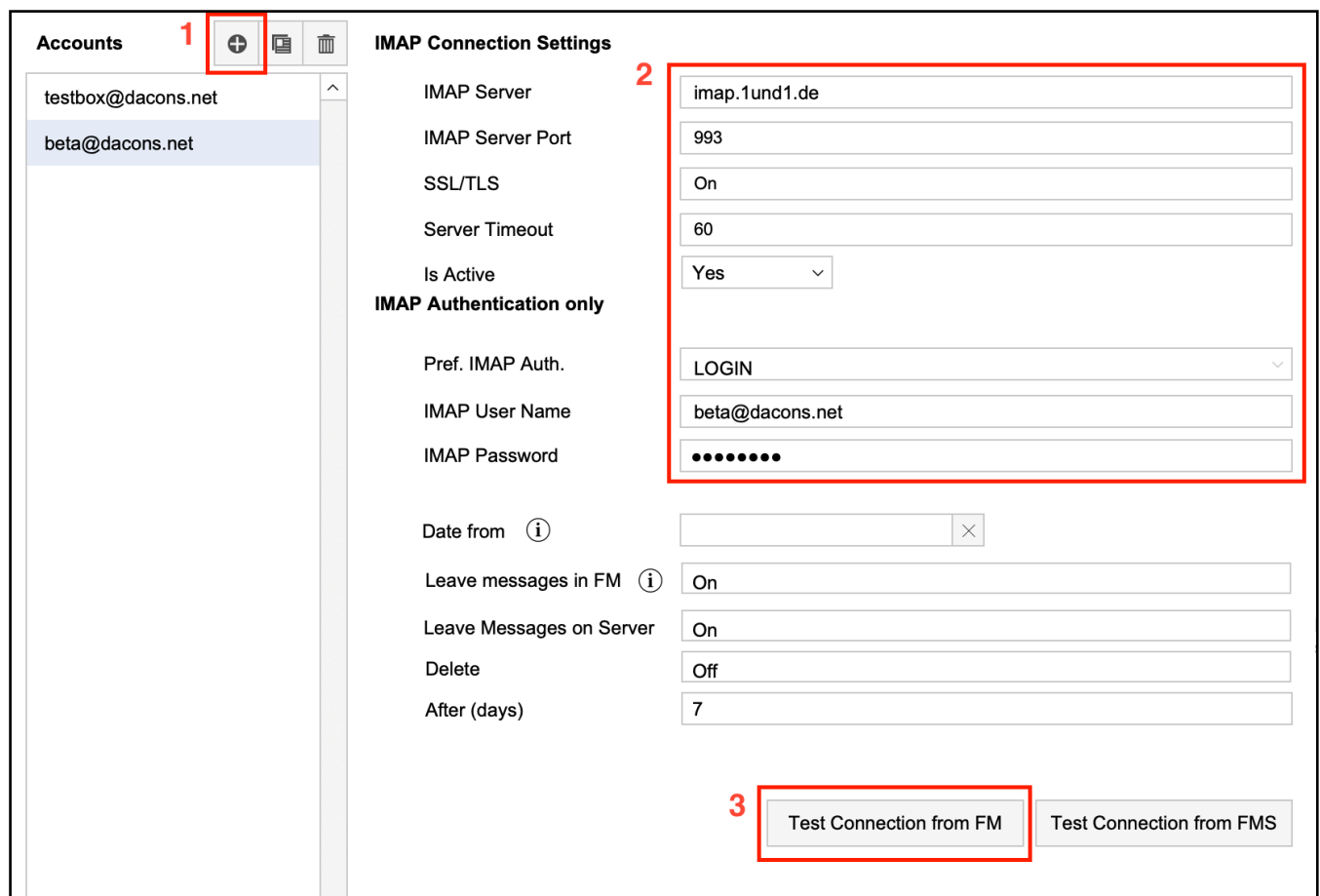
You can now send a message using the “Send” button in the top menu. Or you can go to the “Message Source” tab and click on the “Create Source” button, the plugin will create the message source. If there are any errors with the certificate or private key during the source creation process, a message with an error code will be displayed.

Setting up message download in the Simple Receiving IMAP.fmp12 file

Using the file “Simple Receiving IMAP.fmp12” you can test the downloading of OpenPGP messages.

Open the file “Simple Receiving IMAP.fmp12” and click on the icon  in the upper right corner, this will take you to the account management layout. On the account management layout, click the plus “+” icon, which is located at the top left, in order to create a new account.

Next, fill in the required fields to connect to the IMAP server. Then click the “Test Connection from FM” button to test the connection.



Accounts 1   

IMAP Connection Settings 2

IMAP Server: imap.1und1.de

IMAP Server Port: 993

SSL/TLS: On

Server Timeout: 60

Is Active: Yes

IMAP Authentication only

Pref. IMAP Auth.: LOGIN

IMAP User Name: beta@dacons.net

IMAP Password:

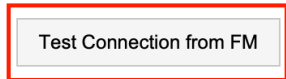
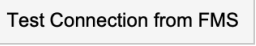
Date from:  

Leave messages in FM : On

Leave Messages on Server: On

Delete: Off

After (days): 7

3  

Next, go to the “End-To-End Encryption” tab and drag your public key file into the “OpenPGP Public Key” field, and your private key file into the “OpenPGP Private Key” field, also into the “OpenPGP Private Key Password” specify the password for the public certificate. Account setup is complete, click the cross icon in the upper right corner.

Last Session Transcript **End-To-End Encryption**

OpenPGP Public Key 0xDA868F5B-pub.asc

OpenPGP Private Key 0xDA868F5B-sec.asc

OpenPGP Private Key Password ••••••••

Now you need to create a sender entry in your contact book. Click the “Contacts” button in the top menu. In the window that opens, click the “+” icon to create a new contact.

Get Mail Delete **1 Contacts** Import Source Mailit 10 Simple Receiving

From <beta> **2 + New Contact**

For a new contact, enter the sender's first name, last name, and email address in the appropriate fields. Go to the "End-To-End Encryption" tab and drag the sender's public key file into the “OpenPGP Public Key” field.

General Home Work End-To-End Encryption

First Name: **Test**

Last Name: **Box**

Email Address: testbox@dacons.net

Photo: [Empty]

General Home Work **End-To-End Encryption**

OpenPGP Public Key testbox@dacons.net-(0xFC3AC11EF3CA080E)-public.asc

Now that you have set up an IMAP account and created one recipient, you can download a message from the server by clicking the “Get Mail” button in the top menu.

The message list has two columns at the end “Decrypt” and “Verify”. If the plugin was able to decode the message or verify the digital signature, “OK” will be displayed in the column. If the plugin fails to perform a decoding operation or digital signature verification, then an error code will be displayed in the column. More information about errors can be found in the plugin log file.

If you do not have a public key when you download the message, then you can add the certificate to your address book and try to decode the message again. To do this, click on the message in the list of messages and go to the "Message Source" tab and click on the "Decrypt" button to decode the message or the "Verify Sign" button to re-verify the digital signature.