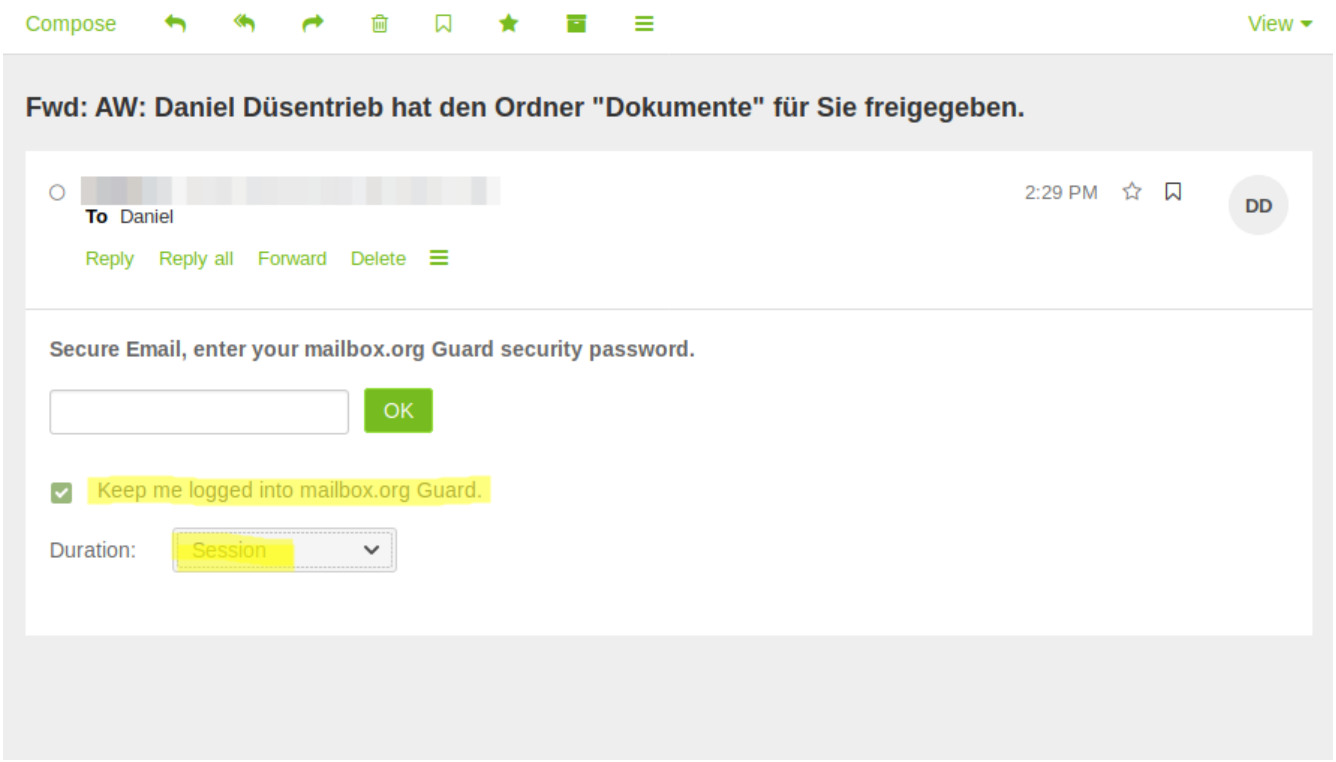
The Encrypted Mailbox

We offer the option of automatically encrypting your incoming e-mails and the sent e-mails as well. This means they are secure in your inbox /sent folder and can be decrypted and read only by you.
This applies only from the point in time on which you activated the Encrypted Mailbox. It's not retroactive.

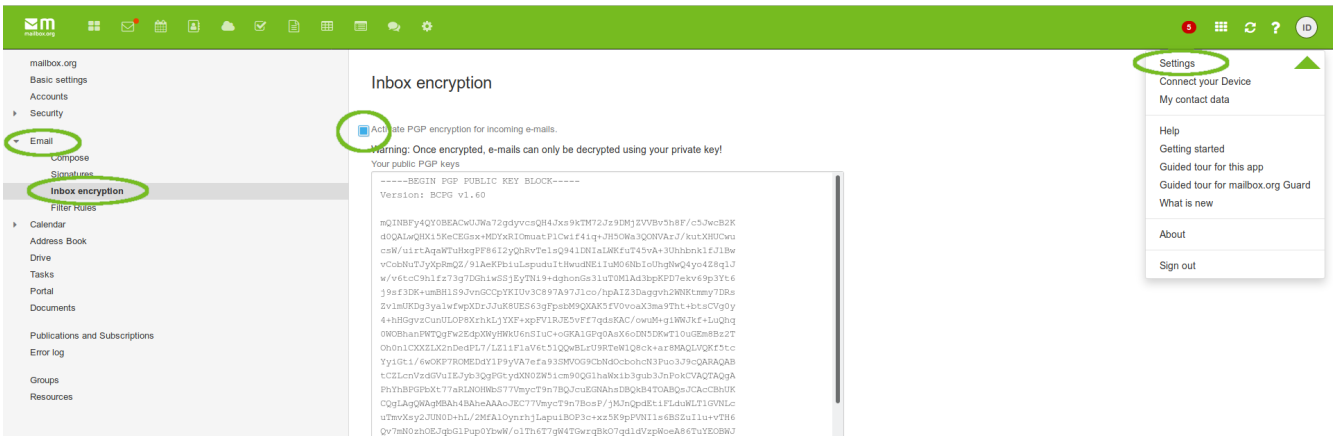
The e-mails contained in the encrypted inbox are encrypted using PGP. As you learned in the first doodle film, the message's sender, recipient, and subject line are not encrypted. This is not possible with any of the encryption methods currently available.

Once you've enable the Encrypted Mailbox, you will always be prompted for the passphrase of you private PGP key if you want to open an encrypted e-mail. You have options to keep you logged in for certain periods of time.



Enabling your mailbox for encryption

You may activate your inbox/sent folder encryption in the ***Settings*** pane at ***Mail - Inbox encryption***. Paste your public key into the text box and enable the option ***Activate PGP encryption for incoming emails***. No need to confirm via any button - it's activated straight away.

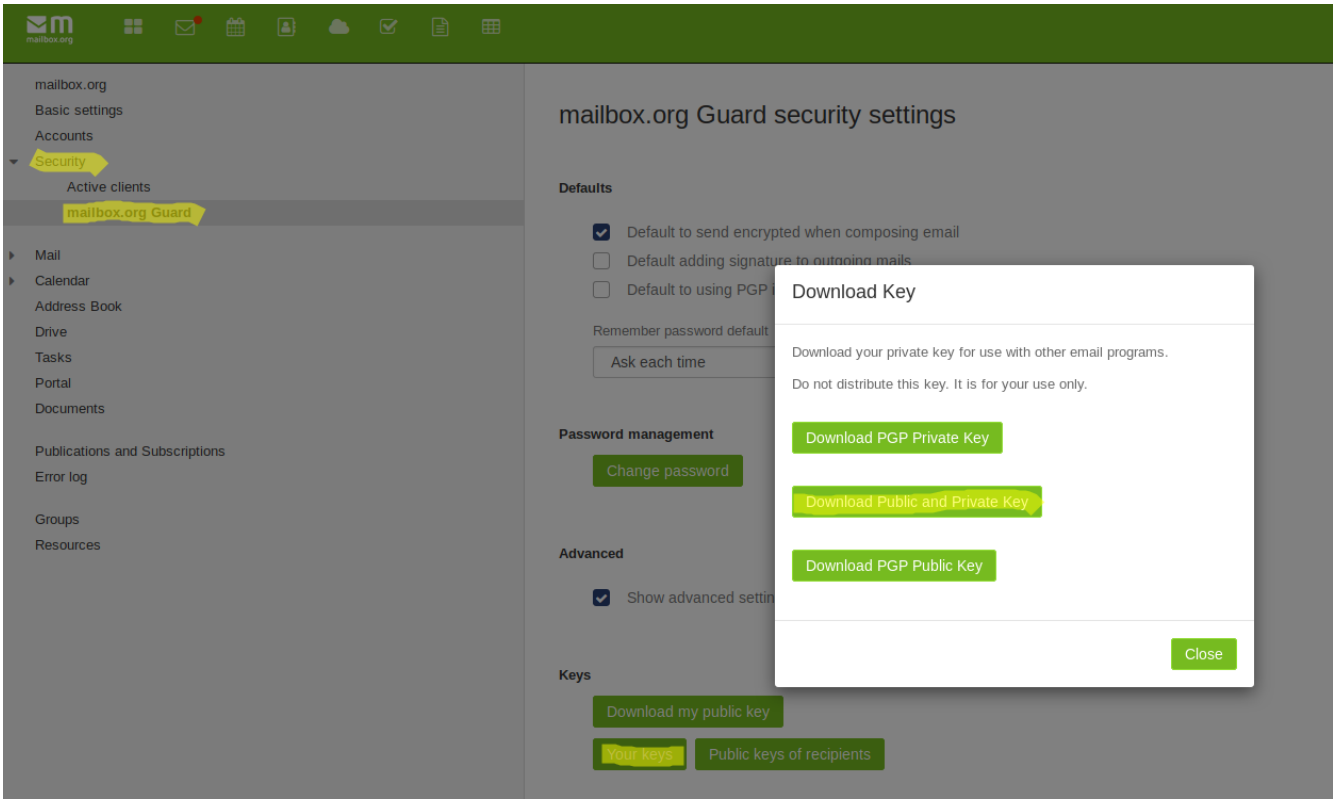


If some error occours, please check, that the key is copied correctly. These settings and the key apply to the encrypted inbox and the sent folder.

The encryption is realized via Sieve Mail filter. Go to ***Mail - Filter Rules*** to find the corresponding rule. Please remember that any new filter rule that you create will be inserted **after** the encrypted mailbox rule. In the settings for filtering rules, there will be shown an error message about unsupported properties. This error is harmless and willl not interfere with any other functions.

Where do I get the PGP key from?

If you have already created a PGP key with our mailbox guard, then you can download both, the private and the public key as follows:



Once you've downloaded the key pair, open it up in a text editor and copy the first part from including "-----BEGIN PGP PUBLIC KEY BLOCK-----" until inculding "-----END PGP PUBLIC KEY BLOCK-----" and paste it into the public PGP key field which is shown in the first screenshot.

Alternatively you can use your own key pair for this. For example, one that has been created with enigmail add-on in Thunderbird. Just make sure not to mix up any keys.

Using the Encrypted Mailbox on other devices

In order to use the encrypted mailbox on your PC with an e-mail client or on a mobile phone e-mail client, make sure to download both, the private and the public PGP key from the webmail interface as per the above description.

Only do this if you consider your device secure. Then use an additional program such as "open key chain" from F-Droid or Enigmail add-on for Thunderbird in order to faciliate access to your encrypted e-mails. In these programs you will be required to import your key pair. Due to the vast field of software combinations in this field, we cannot give further support for this.

Related Articles

- The Encrypted Mailbox
- Read encrypted e-mails with Guard
- How can e-mails be encrypted with PGP
- SMIME supported with encrypted mailbox
- Send encrypted e-mails with Guard