

Installing and using email certificate on Linux

Evolution mail client



(This page was intentionally left blank)

Table of Contents

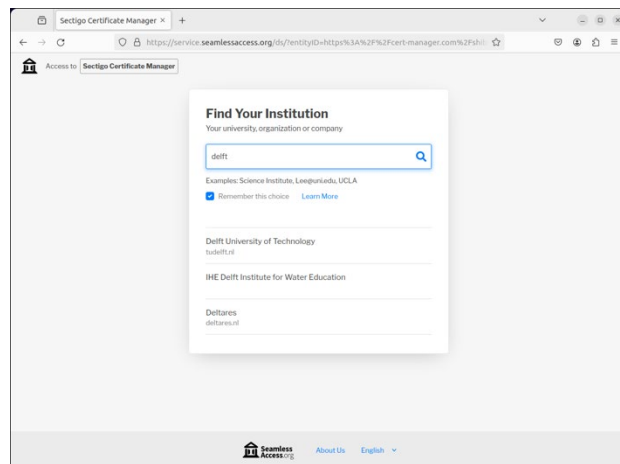
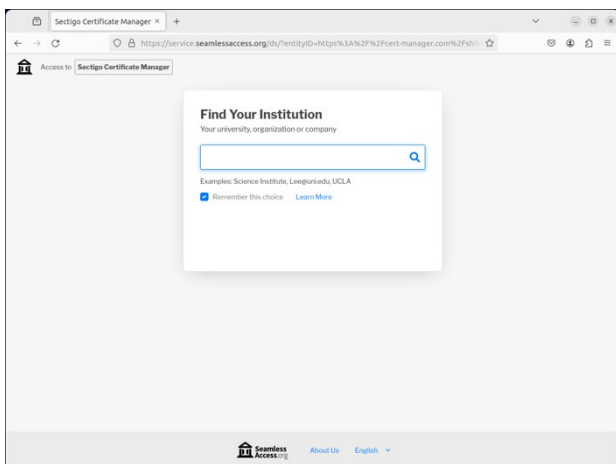
1	Installing and using e-mail certificate on Linux.....	4
1.1	Obtain certificate for Linux	4
1.2	Installing RSA – 2048 / AES256 Key	6
1.3	Setup mail account for using certificate	7

1 Installing and using e-mail certificate on Linux

1.1 Obtain certificate for Linux

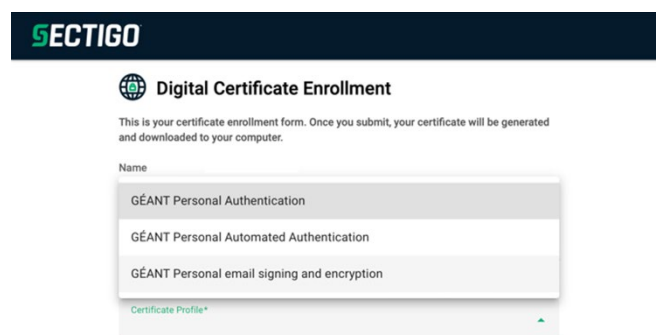
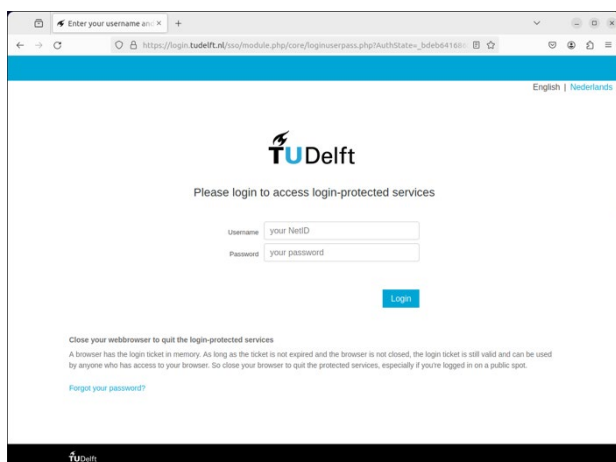
First you have to obtain a certificate with your netid

1. Open a browser and go to <https://edu.nl/sectigo-sso>
2. Find your institution by searching for “Delft”
3. Click on “Delft University of Technology” (tudelft.nl)



4. Fill in you netid and password and login.

5. When you are logged in successfully you see the Digital Certificate Enrollment webpage



6. Choose for GÉANT email Signing and encryption.

7. Choose for the following option to generate a working certificate for macOS

- Term: **365 Days**
- Enrollment Method: **Key Generation**
- Key Type: **RSA - 2048**
- Fill in a password you can remember to install the certificate in a later stadium.
- Choose Key Protection Algorithm: **Secure AES256-SHA256**
- Agree to the terms of the EULA.
- Click "Submit" to generate a certificate and download this certificate.

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name
Organization
Email

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*
GÉANT Personal email signing and encryption

i Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).

Term*
365 days

Enrollment Method
 Key Generation
 CSR

Key Type*
RSA - 2048

Password is required to unlock the certificate file download to protect private key.

Password*
.....

Password Confirmation*
.....

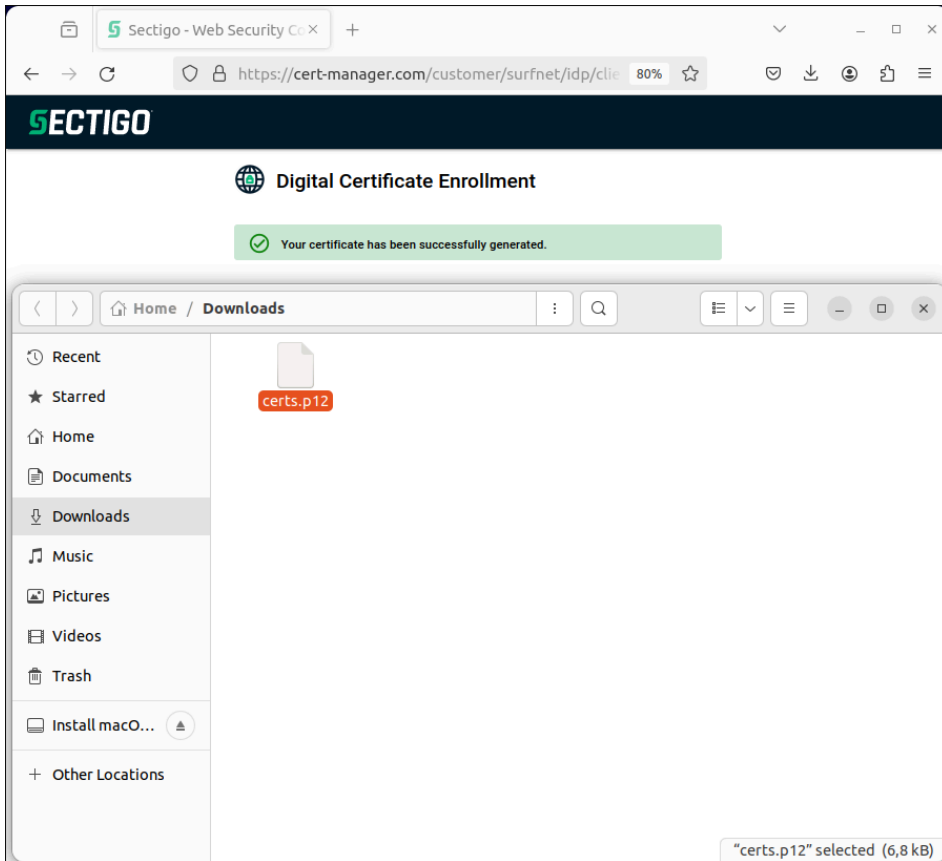
Choose key protection algorithm.

Algorithm
Secure AES256-SHA256

I have read and agree to the terms of the EULA

Submit

8. You now have downloaded a certificate (certs.p12)

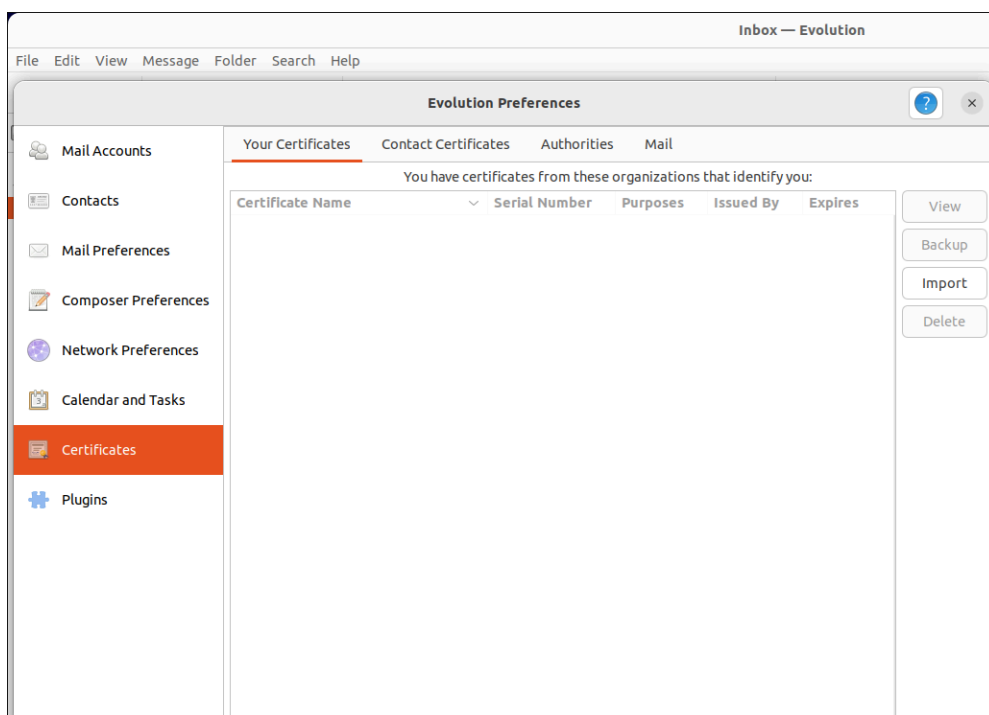


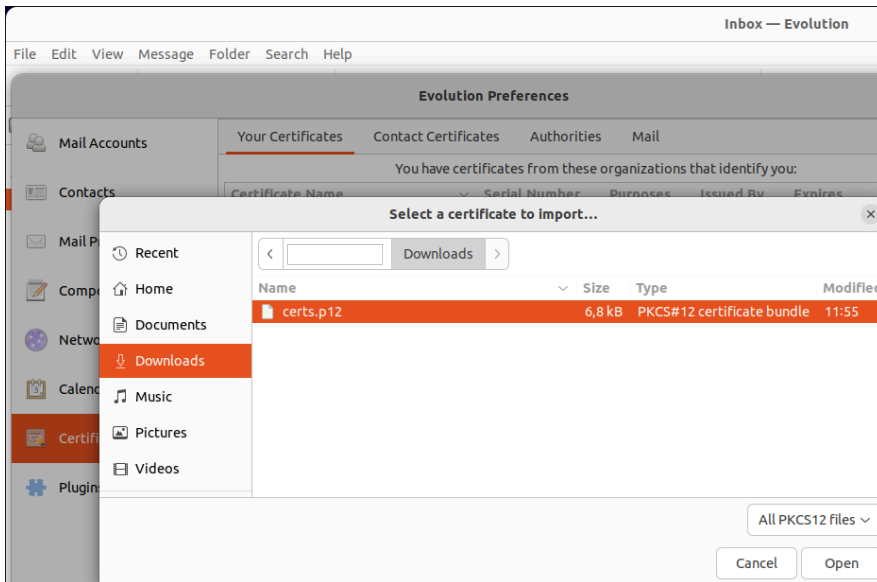
1.2 Installing RSA – 2048 / AES256 Key

9. You can now start your already configured mailclient: **Evolution**

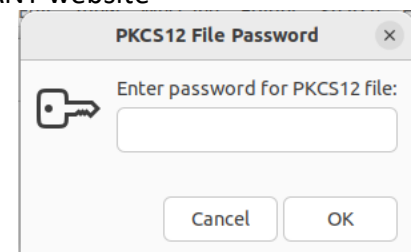
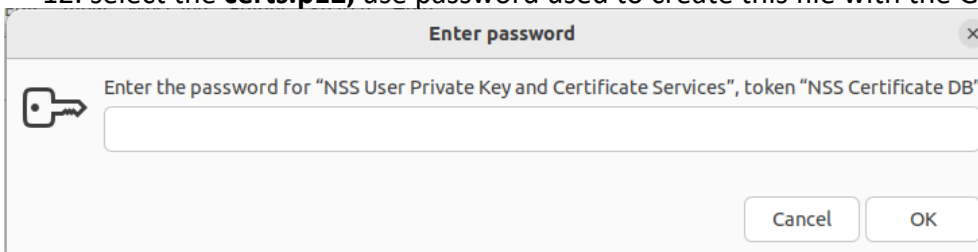
10. From the menu select **Edit** → **Preferences** → **Certificates**

11. install certificate on the left sidebar select **Certificates**
goto tab **Your Certificates** on the right side click **Import**





12. select the **certs.p12**, use password used to create this file with the GÉANT website

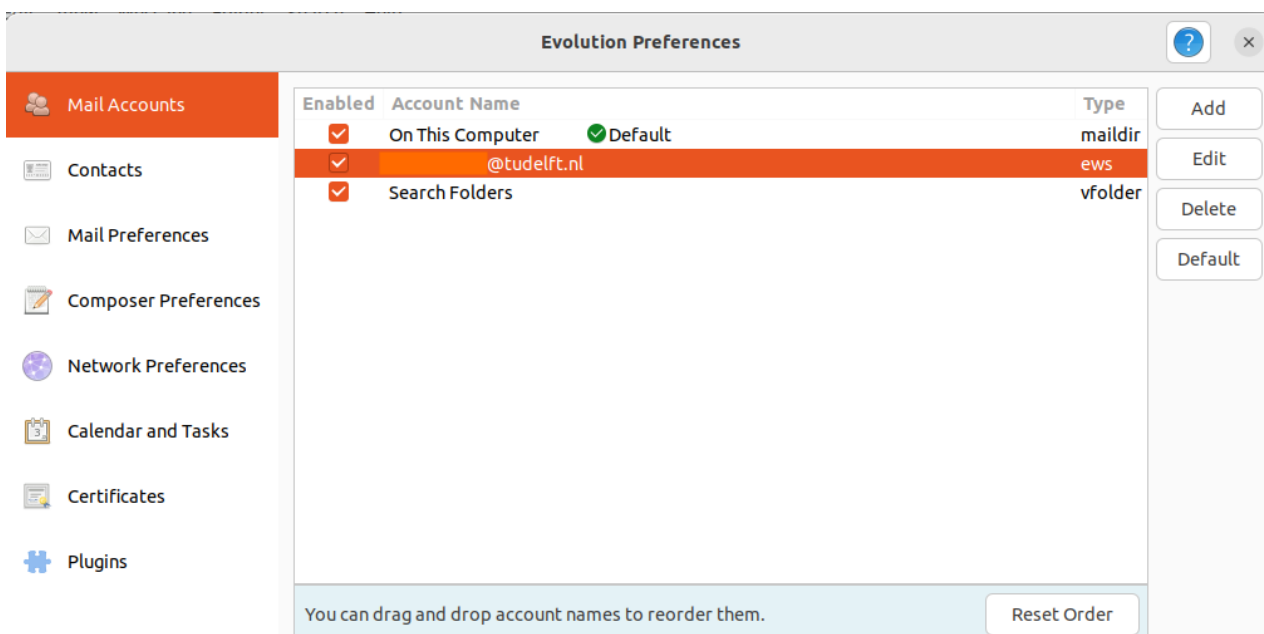


You have now successfully installed the certificate in Evolution, you can now setup Signing and Encryption.

1.3 Setup mail account for using certificate

Setup mail account for using certificate

13. On the left sidebar select **Mail Accounts** select your TU Delft account (Type **ews**) on the right side click **Edit**



14. on the left sidebar select **Security**, click **Select** after **Secure MIME (S/MIME)→Signing certificate**

15. choose your installed certificate from the dropdown menu for **Certificate** and identify your latest certificate by checking the **Expires:** value! Click **OK**

16. click **Select** after **Secure MIME (S/MIME)→Encryption certificate**

choose your installed certificate from the dropdown menu for **Certificate** and identify your latest certificate by checking the **Expires:** value! Click **OK**

The screenshot shows the 'Account Editor' dialog box with the 'Security' tab selected in the left sidebar. The main content area is divided into several sections:

- General**:
 - Do not sign meeting requests (for Outlook compatibility)
- Pretty Good Privacy (OpenPGP)**:
 - OpenPGP Key ID: [text input field]
 - Signing algorithm: [Default v]
 - Always sign outgoing messages when using this account
 - Always encrypt outgoing messages when using this account
 - Always encrypt to myself when sending encrypted messages
 - Always trust keys in my keyring when encrypting
 - Prefer inline sign/encrypt for plain text messages
- Secure MIME (S/MIME)**:
 - Signing certificate: [text input field with red border] [Select] [Clear]
 - Signing algorithm: [Default v]
 - Always sign outgoing messages when using this account
 - Encryption certificate: [text input field] [Select] [Clear]
 - Always encrypt outgoing messages when using this account
 - Always encrypt to myself when sending encrypted messages

At the bottom right, there are 'Cancel' and 'OK' buttons.

Decide on how to use signing and encryption by ticking the appropriate options

You can now sign and/or encrypt e-mail in Evolution.