## Installing and using email certificate on Linux Evolution mail client

\* 1

(This page was intentionally left blank)

### Table of Contents

1	Insta	alling 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.

	cergo - we	ed Security Co A	+			
⇒G	$\bigcirc$	A or https://d	<b>cert-manager.com</b> /customer/surfn	et/idp/clien 80%	☆ ©	اله
ECTIG	n'					
		This is your certifi and downloaded t	icate enrollment form. Once you submit, your c to your computer.	ertificate will be generated		
		Name				
		Organization				
		Email				
		Select your Certifi	cate Profile to enable your enrollment options.			
		Certificate Profile GÉANT Perso	* onal email signing and encryption	•		
		Personal Cer digitally sign ema (but not sign PDF)	rtificate - provides secure email services, and e il communications, as well as sign and protect documents).	nables you to encrypt and some types of document		
		Term* 365 days		•		
		Enrollment Metho	d			
		Key Generation	ation			
		⊖ CSR				
		Kov Tupot		<b>.</b>		
		RSA - 2048				
		RSA - 2048				
		RSA - 2048 Password is requi	red to unlock the certificate file download to pr	otect private key.		
		RSA - 2048 Password is requi	red to unlock the certificate file download to pr	rotect private key.		
		RSA - 2048 Password is requi	red to unlock the certificate file download to pr	rotect private key.		
		Password is requi	ired to unlock the certificate file download to pr	rotect private key.		
		RSA - 2048 Password is requi	red to unlock the certificate file download to pr nation*	rotect private key.		

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

🖻 🔄 Sectigo - We	b Security C○× +	$\sim$	_ 0 ×
$\leftarrow \rightarrow $ C O (	https://cert-manager.com/customer/surfnet/idp/clie 80% 🌣	$\boxtimes$ $+$	: එ ≡
<b>S</b> ECTIGO			
	Digital Certificate Enrollment		
	⊘ Your certificate has been successfully generated.		
	ownloads : Q		- • ×
🕚 Recent			
★ Starred	certs.p12		
습 Home			
Documents			
⊕ Downloads			
🎵 Music			
Pictures			
🛛 Videos			
🗂 Trash			
🔲 Install macO 🔺			
+ Other Locations			
		"certs.p12" of	elected (6.8 kB)
		ceres.p12	

#### 1.2 Installing RSA – 2048 / AES256 Key

- 9. You can now start your already configured mailclient: Evolution
- 10. From the menu select Edit  $\rightarrow$  Preferences  $\rightarrow$  Certificates
- 11. install certificate on the left sidebar select **Certificates** goto tab **Your Certificates** on the right side click **Import**

		Inbox — Evolution
File Edit View Message	Folder Search Help	
		Evolution Preferences
🚇 Mail Accounts	Your Certificates	Contact Certificates Authorities Mail
		You have certificates from these organizations that identify you:
Contacts	Certificate Name	View
Mail Preferences		Backup
Composer Preferences		Import
		Delete
Network Preferences		
📋 Calendar and Tasks		
🧱 Certificates		
<table-of-contents> Plugins</table-of-contents>		

							Inbox — Evol	ution
File	Edit V	iew Message F	older Search Help					
				Evolution Pref	ferences			
22	Mail Accounts		Your Certificates	Contact Certificates	Authorities	Mail		
				You have certificate	es from these org	anizations th	nat identify you:	
	Contac	ts	Certificate Name	<ul> <li>Seri;</li> </ul>	al Number Pi	irnoses	Issued By Exr	lires
				Select a certificate	e to import			×
	Mail Pi	③ Recent	<	Downloads >				
7	Comp	습 Home	Name		<ul> <li>✓ Size</li> </ul>	Туре		Modified
	Netwo	Documents	certs.p12		6,8 kB	PKCS#12	certificate bundle	11:55
	Treewe	Downloads						
3	Calenc	🎵 Music						
	Certifi	Pictures						
#	Plugin	🛛 Videos						
							All PKCS	12 files 🗸
							Cancel	Open

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

Ĩ	Enter password ×	PKCS12 File Password ×
	Enter the password for "NSS User Private Key and Certificate Services", token "NSS Certificate DB"	Enter password for PKCS12 file:
	Cancel OK	Cancel OK

You have now succesfully 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** 

			Evolution Preferences		<b>?</b> ×
2	Mail Accounts	Enabled	Account Name	Type	Add
	Contacts		@tudelft.nl	ews	Edit
	Mail Preferences		Search Folders	vfolder	Delete
1	Composer Preferences				Derivate
۲	Network Preferences				
3,	Calendar and Tasks				
Ę	Certificates				
Ħ	Plugins				
		You can d	rag and drop account names to reorder them.	Reset Order	

- 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** 

	Account Editor	×
Identity	General Do not sign meeting requests (for Outlook compatibility)	
Receiving Email	Pretty Good Privacy (OpenPGP)	
Receiving Options	OpenPGP Key ID:	
Defaults	Signing algorithm: Default ~	
Composing Messages	Always sign outgoing messages when using this account	
Out of Office	Always encrypt outgoing messages when using this account	
Delegates	Always encrypt to myself when sending encrypting Always trust keys in my keyring when encrypting	
Security	Prefer inline sign/encrypt for plain text messages	
	Secure MIME (S/MIME)	
EWS Settings	Signing certificate: Select Cl	ear
	Signing algorithm: Default ~	
	Always sign outgoing messages when using this account	
	Encryption certificate: Select Cl	еаг
	Always encrypt outgoing messages when using this account	
	Always encrypt to myself when sending encrypted messages	
	Cancel	:

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

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